hp StorageWorks

edge switch 2/32 service manual

Part Number: AA-RS2GB-TE

Second Edition (January 2003)

This manual describes the HP StorageWorks Edge Switch 2/32 and attached *HP StorageWorks High Availability Fabric Manager* (*HAFM*) application. For service representatives, it describes diagnostic procedures, repair procedures, and the removal and replacement procedures for field-replaceable units (FRUs). An illustrated parts breakdown is included for all FRUs.

© Hewlett-Packard Company, 2003. All rights reserved.

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard. The information contained in this document is subject to change without notice.

Microsoft, MS-DOS, and Windows, are trademarks of Microsoft Corporation in the U.S. and/or other countries.

All other product names mentioned herein may be trademarks of their respective companies.

Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information is provided “as is” without warranty of any kind and is subject to change without notice. The warranties for Hewlett-Packard Company products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

Printed in the U.S.A.

hp StorageWorks edge switch 2/32 service manual
Second Edition (January 2003)
Part Number: AA-RS2GB-TE

Contents

Contents

About This Manual

Intended Audience xi
Related Documentation xi
Document Conventions xii
Symbols in Text xiii
Symbols on Equipment xiii
Rack Stability xiv
Getting Help xv
HP Technical Support xv
HP Website xv
HP Authorized Reseller xv

General Information

Switch Description 1–2
Switch Management 1–3
Error-Detection, Reporting, and Serviceability Features 1–5
Zoning Feature 1–7
Multi-Switch Fabrics 1–8
Switch Specifications 1–9
Physical Characteristics 1–9
HAFM Server Description 1–11
HAFM Server Specifications 1–12
Ethernet Hub 1–12
Embedded Web Server Interface 1–13
Maintenance Approach 1–13
Remote Workstation Configurations 1–14
Minimum Remote Console Hardware Specifications 1–16
Field Replaceable Units 1–17

SFP Transceivers 1–18
Cooling Fans 1–18
Power Supplies 1–19
Connectors and Indicators 1–19
Initial Machine Load Button 1–19
Ethernet LAN Connector 1–20
Power and System Error LEDs 1–20
FRU Status LEDs 1–20
Maintenance Port 1–21
Software Diagnostic Features 1–21
HAFM Diagnostics 1–21
HAFM Status Symbols 1–23
Hardware View Layout and Function 1–23
Menu Bar 1–24
Product Manager Diagnostics 1–24
Hardware View 1–24
Status Table 1–26
LED Emulation 1–27
Product Manager Status Symbols 1–27
View Tabs 1–27
View Panel 1–28
Status Bar 1–34
Topology Tab 1–37
Zone Set Tab 1–38
HAFM Services Application 1–38
Event Table 1–39
Status Line 1–40
Embedded Web Server Diagnostics 1–41
SNMP Trap Message Support 1–42
E-Mail and Call-Home Support 1–43
Tools and Test Equipment 1–43
Tools Supplied with the Switch 1–44
Tools Supplied by Service Personnel 1–45

Diagnostics

Maintenance Analysis Procedures 2–1
Factory Defaults 2–1
Quick Start 2–1

MAP 0000: Start MAP 2–7
MAP 0100: Power Distribution Analysis 2–26
MAP 0200: POST, Reset, or IPL Failure Analysis 2–32
MAP 0300: Console Application Problem Determination 2–33
MAP 0400: Loss of Console Communication 2–39
MAP 0500: Fan and CTP Failure Analysis 2–58
MAP 0600: Port Failure and Link Incident Analysis. 2–63
MAP 0700: Fabric, ISL, and Segmented Port Problem Determination. 2–79
MAP 0800: Console PC Problem Determination 2–90

Repair Information

Factory Defaults 3–2
Procedural Notes 3–2
Using Log Information. 3–2
HAFM Audit Log 3–3
HAFM Event Log 3–3
Session Log 3–4
Product Status Log. 3–5
Fabric Log 3–5
Audit Log. 3–6
Event Log 3–6
Refresh the Event Log. 3–7
Clear the Event Log 3–7
Hardware Log 3–7
Link Incident Log 3–9
Refresh the Link Incident Log 3–10
Clear the Link Incident Log 3–10
Threshold Alert Log 3–10
Using Views. 3–12
Port List View 3–12
FRU List View. 3–14
Node List View 3–16
Performance View 3–17
Zone Set View 3–17
Performing Port Diagnostics 3–19
Port LEDs 3–19
Hardware View 3–20
Performance View 3–23

Perform Loopback Tests 3–26
Internal Loopback Test 3–26
External Loopback Test 3–28
Perform Channel Wrap Test 3–29
Swapping Ports 3–30
Collecting Maintenance Data 3–32
Clean Fiber-Optic Components 3–33
Power-On Procedure 3–34
Power-Off Procedure 3–35
Reset or IPL the Switch 3–35
Reset the Switch 3–36
IPL the Switch 3–36
Set the Switch Online or Offline 3–37
Set Online State 3–37
Set Offline State 3–38
Block and Unblock Ports 3–39
Block a Port 3–39
Unblock a Port 3–40
Manage Firmware Versions 3–40
Determine a Switch Firmware Version 3–41
Add a Firmware Version 3–41
Modify a Firmware Version Description 3–44
Delete a Firmware Version 3–45
Download a Firmware Version to a Switch 3–46
Manage Configuration Data 3–48
Back Up the Configuration 3–49
Restore the Configuration 3–50
Reset Configuration Data 3–51
Install or Upgrade Software 3–51

FRU Removal and Replacement

Remove and Replace FRUs 4–1
FRUs 4–1
Procedural Notes 4–2
RRP: SFP Transceiver 4–2
Removal 4–2
Replacement 4–3
RRP: Power Supply 4–4

Removal 4–4
Replacement 4–5
RRP: Cooling Fan 4–6
Removal 4–6
Replacement 4–7
RRP: CTP Card — Switch Replacement 4–8
Replacing a Failed Switch 4–8

Illustrated Parts Breakdown

Front-Accessible FRUs 5–1
Rear-Accessible FRUs 5–2
Miscellaneous Parts 5–4

Messages

HAFM Application Messages A–1
Edge-32 Switch Product Manager Messages A–19

Event Codes

System Events (000 through 199) B–2
Power Supply Events (200 through 299) B–14
Fan Module Events (300 through 399) B–17
CTP2 Card Events (400 through 499) B–20
Port Events (500 through 599) B–32
SBAR Events (600 through 699) B–53
Thermal Events (800 through 899) B–60

Glossary

Index

Figures

1–1 Switch, HAFM server, and Ethernet Hub 1–2
1–2 Out-of-Band Product Management 1–4
1–3 Inband Product Management 1–5
1–4 HAFM server 1–11
1–5 12-Port Ethernet Hub 1–13
1–6 Typical Network Configuration (One Ethernet Connection) 1–15

1–7 Typical Network Configuration (Two Ethernet Connections) 1–15
1–8 Edge Switch 2/32 (front view). 1–17
1–9 Edge Switch 2/32 (rear view) 1–18
1–10 Product View 1–22
1–11 Hardware View 1–25
1–12 Hardware View 1–28
1–13 Port List View 1–30
1–14 FRU List View. 1–31
1–15 Node List View 1–32
1–16 Performance View 1–33
1–17 Fabrics View — Topology Tab 1–37
1–18 Fabrics View — Zone Sets Tab. 1–38
1–19 HAFM Services Window 1–39
1–20 Multi-mode and Single-mode Loopback Plugs 1–44
1–21 Fiber-Optic Protective Plug 1–44
1–22 Null Modem Cable 1–45
3–1 HAFM Event Log 3–4
3–2 Product Status Log. 3–5
3–3 Switch Event Log 3–6
3–4 Hardware Log 3–8
3–5 Link Incident Log 3–9
3–6 Threshold Alert Log 3–11
3–7 Port List View 3–13
3–8 FRU List View. 3–15
3–9 Node List View 3–16
3–10 Zone Sets View 3–18
3–11 Hardware View 3–20
3–12 Port Properties Dialog Box 3–21
3–13 Performance View 3–24
3–14 Port Diagnostics Dialog Box 3–27
3–15 Channel Wrap On for Port n Dialog Box 3–30
3–16 Swap Ports Dialog Box 3–31
3–17 Save Data Collection Dialog Box 3–32
3–18 Data Collection Dialog Box 3–33
3–19 Clean Fiber-Optic Components 3–34
3–20 Information dialog box 3–37
3–21 Online State dialog box 3–38
3–22 Block Port n dialog box 3–39

3–23 Unblock Port n dialog box 3–40
3–24 Firmware Library dialog box 3–41
3–25 Firmware Library dialog box 3–42
3–26 New Firmware Version dialog box 3–43
3–27 New Firmware Description dialog box 3–43
3–28 Firmware Library dialog box 3–44
3–29 Modify Firmware Description dialog box 3–44
3–30 Firmware Library dialog box 3–45
3–31 Firmware Library dialog box 3–47
3–32 Send Firmware confirmation box 3–47
3–33 Send firmware complete message 3–48
3–34 Backup and Restore Configuration dialog box 3–49
3–35 Backup Complete dialog box 3–49
3–36 Backup and Restore Configuration dialog box 3–50
3–37 Warning message box 3–50
3–38 Restore Complete dialog box 3–51
3–39 Run dialog box 3–53
3–40 HAFM dialog box 3–53
5–1 Front-Accessible FRUs 5–1
5–2 Rear-Accessible FRUs 5–3

Tables

1–1 Status Symbols 1–23
1–2 Operating Status — Status Bar and Switch Status Table 1–35
1–3 HAFM Services Status Symbols 1–41
2–1 Factory-Set Defaults 2–1
2–2 MAP Summary 2–2
2–3 Event Codes versus Maintenance Action 2–2
3–1 Factory-Set Defaults 3–2
4–1 ESD Requirements 4–1
5–1 Front-Accessible FRU Parts List 5–2
5–2 Rear-Accessible FRU Parts List 5–3
5–3 Miscellaneous Parts 5–4

About This Manual

This manual describes the service procedures for the HP StorageWorks Edge Switch 2/32.

Intended Audience

This publication is intended for service personnel, and any individuals who monitor, configure, and repair the Edge Switch 2/32.

Related Documentation

For a list of corresponding documentation included with this product, see the "Related Documents" section of the *hp StorageWorks edge switch release notes*.

For the latest information, documentation, and firmware releases, please visit the HP StorageWorks website:

http://h18006.www1.hp.com/storage/saninfrastructure.html

For information about Fibre Channel standards, visit the Fibre Channel Industry Association website, located at http://www.fibrechannel.org.

Document Conventions

The conventions included in Table 1 apply.

Table 1: Document Conventions

Element	Convention
Cross-reference links	Blue text: Figure 1
Key names, menu items, buttons, and dialog box titles	**Bold**
File names, application names, and text emphasis	*Italics*
User input, command names, system responses (output and messages)	`Monospace font` `COMMAND NAMES` are uppercase unless they are case sensitive
Variables	*`Monospace, italic font`*
Website addresses	Sans serif font (http://thenew.hp.com)

Symbols in Text

These symbols may be found in the text of this manual. They have the following meanings.

WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or loss of life.

CAUTION: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or data.

IMPORTANT: Text set off in this manner presents clarifying information or specific instructions.

NOTE: Text set off in this manner presents commentary, sidelights, or interesting points of information.

Symbols on Equipment

Any enclosed surface or area of the equipment marked with these symbols indicates the presence of electrical shock hazards. Enclosed area contains no operator serviceable parts.

WARNING: To reduce the risk of injury from electrical shock hazards, do not open this enclosure.

Any RJ-45 receptacle marked with these symbols indicates a network interface connection.

WARNING: To reduce the risk of electrical shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.

Any surface or area of the equipment marked with these symbols indicates the presence of a hot surface or hot component. Contact with this surface could result in injury.

WARNING: To reduce the risk of injury from a hot component, allow the surface to cool before touching.

Power supplies or systems marked with these symbols indicate the presence of multiple sources of power.

WARNING: To reduce the risk of injury from electrical shock, remove all power cords to completely disconnect power from the power supplies and systems.

Any product or assembly marked with these symbols indicates that the component exceeds the recommended weight for one individual to handle safely.

WARNING: To reduce the risk of personal injury or damage to the equipment, observe local occupational health and safety requirements and guidelines for manually handling material.

Rack Stability

WARNING: To reduce the risk of personal injury or damage to the equipment, be sure that:

- **The leveling jacks are extended to the floor.**
- **The full weight of the rack rests on the leveling jacks.**
- **In single rack installations, the stabilizing feet are attached to the rack.**
- **In multiple rack installations, the racks are coupled.**
- **Only one rack component is extended at any time. A rack may become unstable if more than one rack component is extended for any reason.**

Getting Help

If you still have a question after reading this manual, contact an HP authorized service provider or access our website: http://thenew.hp.com.

HP Technical Support

In North America, call technical support at 1-800-652-6672, available 24 hours a day, 7 days a week.

NOTE: For continuous quality improvement, calls may be recorded or monitored.

Outside North America, call technical support at the nearest location. Telephone numbers for worldwide technical support are listed on the HP website under support: http://thenew.hp.com/country/us/eng/support.html.

Be sure to have the following information available before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

HP Website

The HP website has the latest information on this product, as well as the latest drivers. Access storage at: http://thenew.hp.com/country/us/eng/prodserv/storage.html. From this website, select the appropriate product or solution.

HP Authorized Reseller

For the name of your nearest HP Authorized Reseller:

- In the United States, call 1-800-345-1518
- In Canada, call 1-800-263-5868
- Elsewhere, see the HP website for locations and telephone numbers: http://thenew.hp.com.

1

General Information

The HP StorageWorks Edge Switch 2/32 provides dynamic switched connections between Fibre Channel servers and devices in a storage area network (SAN) environment. SANs introduce the concept of server-to-device networking and multi-switch fabrics, eliminate requirements for dedicated connections, and enable the enterprise to become data centric.

A SAN provides speed, high capacity, and flexibility for the enterprise, and is primarily based upon Fibre Channel architecture. The switch implements Fibre Channel technology that provides a bandwidth of 2.125 gigabits per second, redundant switched data paths, a scalable number of active ports, and long transmission distances (up to 35 kilometers).

This chapter describes the switch and attached HP StorageWorks High Availability Fabric Manager (HAFM) server. The chapter specifically discusses:

- Switch management, error-detection and reporting features, serviceability features, zoning, multi-switch fabrics, and specifications.
- The HAFM server and minimum hardware specifications.
- Remote workstation configurations and hardware specifications.
- Maintenance approach.
- Field-replaceable units (FRUs).
- Connectors and indicators.
- Software diagnostic features.
- Tools and test equipment.

Switch Description

The switch can be installed on a table or desk top, or mounted in an equipment cabinet or in any standard equipment rack.

Multiple switches and the HAFM server communicate on a local area network (LAN) through one or more 10/100Base-T Ethernet hubs. One or more 12-port Ethernet hubs are optional and can be ordered with the switch. Up to three hubs are daisy-chained as required to provide additional Ethernet connections as more switches (or other HP managed products) are installed on a customer network.

Figure 1–1 illustrates the switch, HAFM server, and Ethernet hub.

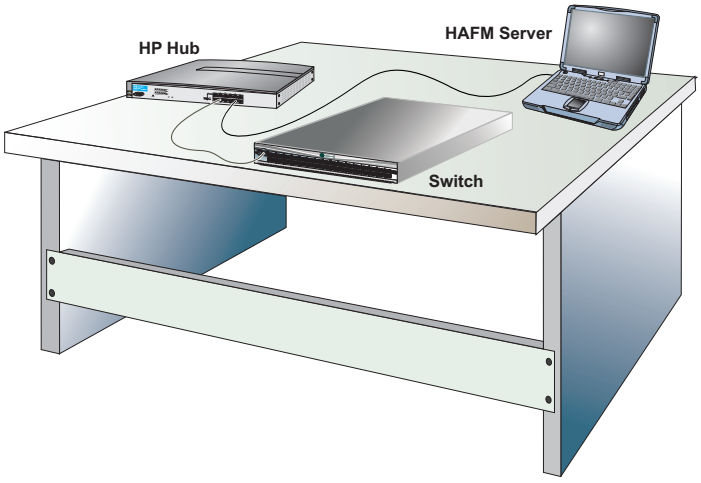


Figure 1–1: Switch, HAFM server, and Ethernet Hub

The switch provides dynamic switched connections for servers and devices, supports mainframe and open-systems interconnection (OSI) computing environments, and provides data transmission and flow control between device node ports (N_Ports) as dictated by the Fibre Channel Physical and Signaling Interface (FC-PH 4.3). Through interswitch links (ISLs), the switch can connect additional switches to form a Fibre Channel multi-switch fabric.

The switch provides connectivity for devices manufactured by multiple original equipment manufacturers (OEMs). To determine if an OEM product can communicate through connections provided by the switch, or if communication restrictions apply, refer to the supporting publications for the product or contact your HP marketing representative

Switch Management

Out-of-band (non-Fibre Channel) management access to HP products is provided through an Ethernet LAN connection to a switch front panel. The following out-of-band management access methods are provided:

- Management through the *HAFM* application. The *HAFM* application includes the *Edge Switch 2/32 Product Manager* application. This GUI resides on the HAFM server and provides a single point of management for all directors and switches.

  Operators at remote workstations can connect to the HAFM server through the local *HAFM* application and associated *Product Manager* applications to manage and monitor switches controlled by the HAFM server. A maximum of nine concurrent users (including a local user) can log in to the *HAFM* application.

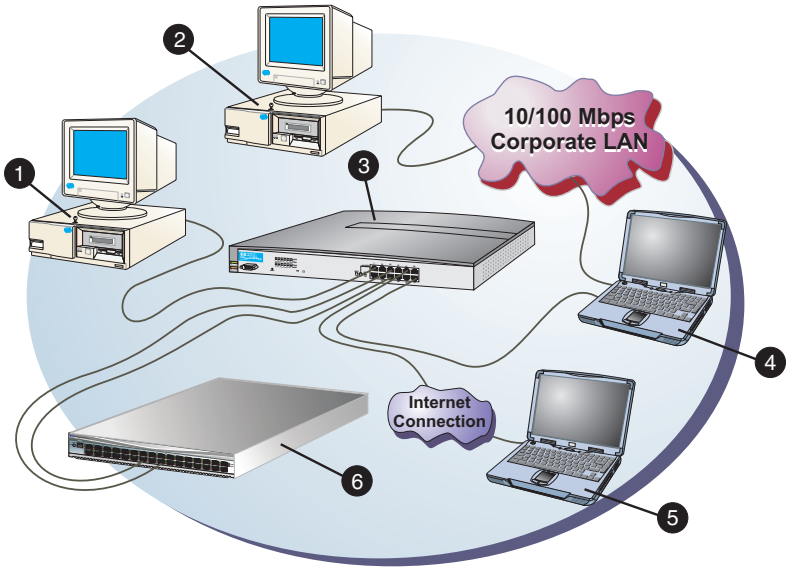
- Management using simple network management protocol (SNMP). An SNMP agent is implemented through the *HAFM* application that allows administrators on SNMP management workstations to access product management information using any standard network management tool. Administrators can assign Internet Protocol (IP) addresses and corresponding community names for up to six SNMP workstations functioning as SNMP trap message recipients.

- Management through the Internet using the EWS interface installed on the director or switch. This interface supports configuration, statistics monitoring, and basic operation of the product, but does not offer all the capabilities of the corresponding *Product Manager* application. Administrators launch the web server interface from a remote PC by entering the product's IP address as the Internet uniform resource locator (URL), then entering a user name and password at a login screen. The PC browser then becomes a management console.

- Management through a customer-supplied remote workstation communicating with the HAFM server through a corporate intranet.

- Management through the command line interface (CLI). The CLI allows you to access many *HAFM* and *Product Manager* applications while entering commands during a telnet session with the switch. The primary purpose of the CLI is to automate management of a large number of switches using scripts. The CLI is not an interactive interface; no checking is done for pre-existing conditions and no prompts display to guide users through tasks. Refer to the *hp StorageWorks CLI reference guide for directors and edge switches*.

Figure 1–2 illustrates an example of out-of-band product management. In the figure, the managed product is an Edge Switch 2/32.



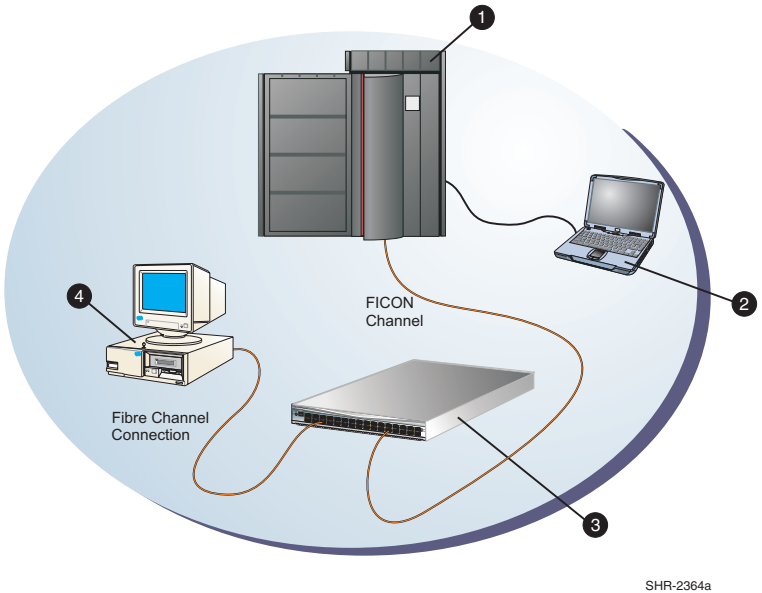
❶	SNMP management workstation	❹	HAFM server
❷	Remote user workstation	❺	Web browser
❸	HP Ethernet hub	❻	Edge Switch 2/32

Figure 1–2: Out-of-Band Product Management

The following inband management access methods are provided as options:

- Management through the product's open-system management server (OSMS) that communicates with an application client. The application resides on an open-systems interconnection (OSI) device attached to a switch port, and communicates using Fibre Channel common transport (FC-CT) protocol. Product operation, port connectivity, zoning, and fabric control are managed through a device-attached console.
- Management through the product's Fibre Connection (FICON) management server (FMS) that communicates with the IBM System Automation for OS/390 (SA OS/390) operating system. The operating system resides on an IBM System/390 or zSeries 900 Parallel Enterprise server attached to a director or switch port, and communicates through a FICON channel. Control of connectivity and statistical product monitoring are provided through a host-attached console.

Figure 1–3 on page 1-5 illustrates inband product management. In the figure, the managed product is an Edge Switch 2/32. The figure shows the following elements:



❶ S/390 or zSeries 900 parallel Enterprise server
❷ Host-attached console
❸ Edge Switch 2/32
❹ OSI server

Figure 1–3: Inband Product Management

Error-Detection, Reporting, and Serviceability Features

The switch provides the following error-detection, reporting, and serviceability features:

- Light-emitting diodes (LEDs) on switch FRUs and adjacent to Fibre Channel ports that provide visual indicators of hardware status or malfunctions.
- System and threshold alerts, event logs, audit logs, link incident logs, threshold alert logs, and hardware logs that display switch, Ethernet link, and Fibre Channel link status at the HAFM server or on a remote workstation.

- Diagnostic software that performs power-on self-tests (POSTs) and port diagnostics (internal loopback, external loopback, and Fibre Channel (FC) wrap tests). The FC wrap test applies only when the switch is configured to operate in S/390 mode.
- Automatic notification of significant system events (to support personnel or administrators) through e-mail messages or the call-home feature.
- An internal modem in the HAFM server for HP call-home support

  NOTE: For directors and switches installed in some legacy environments, call-home notification requires installation of HP Proactive Service software. This service is offered at no additional charge for subsystems covered under an on-site warranty or on-site storage hardware support contract. To register or order Proactive Service software, contact your HP customer service representative.
- An RS-232 maintenance port at the rear of the switch (port access is password protected) that enables installation or service personnel to change the switch's internet protocol (IP) address, subnet mask, and gateway address; or to run diagnostics and isolate system problems through a local or remote terminal.
- Redundant FRUs; small form factor pluggable (SFP) optical transceivers, power supplies, and cooling fans that are removed or replaced without disrupting switch or Fibre Channel link operation.
- A modular design that enables quick removal and replacement of FRUs without tools or equipment.
- Concurrent port maintenance. SFPs and Fiber-optic cables are removed and attached to ports without interrupting other ports or switch operation.
- Beaconing to assist service personnel in locating a specific port or switch. When port beaconing is enabled, the amber LED associated with the port flashes. When unit beaconing is enabled, the system error indicator on the front panel flashes. Beaconing does not affect port or switch operation.
- Data collection through the *Product Manager* application to help isolate system problems. The data includes a memory dump file and audit, hardware, and engineering logs.
- Status monitoring of redundant FRUs and alternate Fibre Channel data paths to ensure continued switch availability in case of failover. The *HAFM* application queries the status of each backup FRU daily. A backup FRU failure is indicated by an illuminated amber LED.

- Simple network management protocol (SNMP) management using the Fibre Alliance MIB that runs on the HAFM server. Up to 12 authorized management workstations can be configured through the *HAFM* application to receive unsolicited SNMP trap messages. The trap messages indicate operational state changes and failure conditions.
- SNMP management using the Fibre Channel Fabric Element MIB, transmission control protocol/internet protocol (TCP/IP) MIB-II definition (RFC 1213), and a product-specific MIB, all of which run on each switch. Up to 12 authorized management workstations can be configured through the *Product Manager* application to receive unsolicited SNMP trap messages. The trap messages indicate switch operational state changes and failure conditions.

NOTE: For more information about SNMP support provided by HP products, refer to the *hp StorageWorks SNMP reference guide for directors and edge switches*.

Zoning Feature

The switch supports a name server zoning feature that partitions attached devices into restricted-access groups called zones. Devices in the same zone can recognize and communicate with each other through switched port-to-port connections. Devices in separate zones cannot communicate with each other.

Zoning is configured by authorizing or restricting access to name server information associated with device N_Ports that attach to switch fabric ports (F_Ports). A zone member is specified by the port number to which a device is attached, or by the eight-byte (16-digit) worldwide name (WWN) assigned to the host bus adapter (HBA) or Fibre Channel interface installed in a device. A device can belong to multiple zones.

CAUTION: If zoning is implemented by port number, a change to the switch fiber-optic cable configuration disrupts zone operation and may incorrectly include or exclude a device from a zone.

If zoning is implemented by WWN, removal and replacement of a device HBA or Fibre Channel interface (thereby changing the device WWN) disrupts zone operation and may incorrectly include or exclude a device from a zone.

In Open Fabric mode, only zoning by WWN is supported. Zoning by port numbers is not.

Zones are grouped into zone sets. A zone set is a group of zones that is enabled (activated) or disabled across all switches in a multi-switch fabric. Only one zone set per fabric can be enabled at one time.

Multi-Switch Fabrics

A Fibre Channel topology that consists of one or more interconnected switches or switch elements is called a fabric. Operational software provides the ability to interconnect switches (through expansion port (E_Port) connections, also referred to as ISL) to form a multi-switch fabric. The data transmission path through the fabric is typically determined by fabric elements and is user-transparent. Subject to zoning restrictions, devices attached to any interconnected switch can communicate with each other through the fabric.

Because a multi-switch fabric is typically complex, maintenance personnel should be aware that several factors can degrade fabric performance or cause connectivity failures. These factors include:

- **Domain ID assignment —** Each switch in a fabric is identified by a unique domain ID that ranges from 1 through 31. A domain ID of 0 is invalid. If two operational fabrics join, they determine if any domain ID conflicts exist between the fabrics. If one or more conflicts exist, the E_Ports that form the interswitch link (ISL) segment to prevent the fabrics from joining.
- **Zoning —** In a multi-switch fabric, zoning is configured on a fabric-wide basis, and any change to the zoning configuration is applied to all switches in the fabric. To ensure zoning is consistent across a fabric, the following rules are enforced when two fabrics (zoned or unzoned) join:
  - — **Fabric A unzoned and Fabric B unzoned —** The fabrics join successfully, and the resulting fabric remains unzoned.
  - — **Fabric A zoned and Fabric B unzoned —** The fabrics join successfully, and fabric B automatically inherits the zoning configuration from fabric A.
  - — **Fabric A unzoned and Fabric B zoned —** The fabrics join successfully, and fabric A automatically inherits the zoning configuration from fabric B.
  - — **Fabric A zoned and Fabric B zoned —** The fabrics join successfully only if the zone configurations can be merged. If the fabrics cannot join, the connecting ports segment and the fabrics remain independent.

  Zone configurations for two fabrics are compatible (the zones can join) if the active zone set name is identical for each fabric, and if zones with the same name have identical elements.
- **Port segmentation —** When an ISL activates, the switches exchange operating parameters to determine if they are compatible and can join to form a single fabric. If incompatible, the connecting E_Port at each switch segments to prevent

the creation of a single fabric. A segmented link transmits only Class F traffic; the link does not transmit Class 2 or Class 3 traffic. The following conditions cause ports to segment:

— **Incompatible operating parameters —** either the resource allocation time-out value (*R_A_TOV*) or error-detect time-out value (*E_D_TOV*) is inconsistent between switches. To prevent port segmentation, the same *E_D_TOV* and *R_A_TOV* must be specified for each switch.

— **Duplicate domain IDs —** one or more domain ID conflicts are detected.

— **Incompatible zoning configurations —** zoning configurations for the switches are not compatible.

— **Build fabric protocol error —** a protocol error is detected during the process of forming the fabric.

— **No principal switch —** no switch in the fabric is capable of becoming the principal switch.

NOTE: At least one director or switch in a multi-switch fabric must be set to either principal or default, making it capable of becoming principal switch. If all directors and switches are set to never principal, all ISLs will segment (Reason code 05).

— **Unresponsive switch —** Each switch in a fabric periodically verifies operation of all attached switches. An ISL segments if the attached switch does not respond to a verification request.

— **ELP retransmission failure timeout-**a switch that exhibits a hardware failure or connectivity problem cannot transmit or receive Class F frames. The switch did not receive a response to multiple exchange link protocol (ELP) frames, did not receive a fabric login (FLOGI) frame, and cannot join an operational fabric.

Switch Specifications

This section lists the physical characteristics, storage and shipping environment, operating environment, and service clearances for the switch.

Physical Characteristics

Dimensions:

Height: 2.55 inches (6.47 centimeters)

Width: 17.5 inches (44.5 centimeters)

Depth: 25.1 inches (63.75 centimeters)

Weight: 34 pounds (15.4 kilograms)

Power Requirements:

Input voltage: 100 to 230 VAC

Input Frequency: 47 to 63 Hz

Plan for single phase or phase-to-phase connections and 5-ampere dedicated service

Airflow Clearance in Rack:

Sides: None

Top and Bottom: None

Front and Rear: 3.0 inches (7.6 centimeters)

Heat Dissipation:

836 BTU/Hr

Shock and Vibration Tolerance:

60 Gs for 10 milliseconds without nonrecoverable errors

Acoustical Noise:

70 dB “A” scale

Inclination:

10° maximum

Storage and Shipping Environment

Protective packaging must be provided to protect the switch under all shipping methods (domestic and international).

Shipping temperature:

-40° F to 140° F (-40° C to 60° C)

Storage temperature:

34° F to 140° F (1° C to 60° C)

Shipping relative humidity:

5% to 100%

Storage relative humidity:

5% to 80%

Maximum wet-bulb temperature:

84° F (29° C)

Altitude:

40,000 feet (12,192 meters)

Operating Environment

Temperature:

40° F to 104° F (4° C to 40° C)

Relative humidity:

8% to 80%

Maximum wet-bulb temperature:

81° F (27° C)

Altitude:

10,000 feet (3,048 meters)

HAFM Server Description

The HAFM server (Figure 1–1) is a notebook personal computer (PC) that provides a central point of control for up to 48 LAN-connected directors or edge switches.

Figure 1–4: HAFM server

The server is mounted in a slide-out drawer in an HP-supplied equipment rack. The HAFM server or Internet access to the Embedded Web Server interface is required to install, configure, and manage the switch.

Although a configured switch operates normally without HAFM server intervention, an attached server should operate at all times to monitor switch operation, log events and configuration changes, and report failures.

The HAFM server provides an auto-detecting 10/100 Mbps LAN connection, provided by an internal Ethernet adapter card. This LAN port attaches to the customer's public intranet to allow access from remote user workstations. An optional Ethernet adapter card (not supplied by HP) can be installed in the personal computer memory card international association (PCMCIA) slot to provide a connection to a private LAN segment for dedicated switch communication.

HAFM Server Specifications

The following list summarizes hardware specifications for the HAFM server notebook platform. Current platforms may ship with more enhanced hardware, such as a faster processor, additional random- access memory (RAM), or a higher-capacity hard drive or removable disk drive.

- HP OmniBook 6200 PC with color monitor, keyboard, keyboard-mounted trackpad (mouse), and U. S. power cord.
- Intel® Pentium III™ processor with an 800 megahertz (MHz) or greater clock speed, running the Microsoft Windows 2000 operating system.
- Eighteen gigabyte (GB) or greater internal hard drive.
- 160 megabyte (MB) or greater RAM.
- Removable DVD/CD-ROM drive.
- Removable 100 MB disk (Zip®) drive.
- 56K internal modem.
- One internal 10/100 Mbps Ethernet adapter with RJ-45 connector (provides public LAN interface to switches and remote clients).

Ethernet Hub

The HAFM server and managed switches connect through a rack- mounted 10/100 Base-T Ethernet hub. Figure 1–5 illustrates the optional 12-port hub.

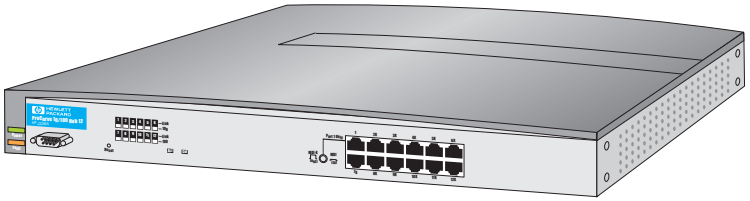


Figure 1–5: 12-Port Ethernet Hub

Embedded Web Server Interface

Administrators or operators with a browser-capable PC and an Internet connection can monitor and manage the switch through an Embedded Web Server interface. The application provides a graphical user interface (GUI) similar to the *Product Manager* application, and supports switch configuration, statistics monitoring, and basic operation.

Maintenance Approach

Whenever possible, the maintenance approach instructs service personnel to perform fault isolation and repair procedures without degrading or interrupting operation of the switch, attached devices, or associated applications. Switch fault isolation begins when one or more of the following occur:

- System event information displays at the attached HAFM server, a remote workstation communicating with the HAFM server, or the Embedded Web Server interface.
- LEDs on the switch front panel or FRUs illuminate to indicate a hardware malfunction.
- An unsolicited SNMP trap message is received at a management workstation, indicating an operational state change or failure.
- Notification of a significant system event is received at a designated support center through an e-mail message or the call-home feature.

System events can be related to a:

- Switch or HAFM server failure (hardware or software).
- Ethernet LAN communication failure between the switch and HAFM server
- Link failure between a port and attached device.

- ISL failure or segmentation of an E_port.

Fault isolation and service procedures vary depending on the system event information provided. Fault isolation and related service information is provided through maintenance analysis procedures (MAPs) documented in Chapter 3. MAPs consist of step-by-step procedures that prompt service personnel for information or describe a specific action to be performed. MAPs provide information to interpret system event information, isolate a switch failure to a single FRU, remove and replace the failed FRU, and verify switch operation. The fault isolation process normally begins with "MAP 0000: Start MAP" on page 2-7.

Ensure the correct switch is selected for service (if the HAFM server manages multiple switches or other HP products) by enabling unit beaconing at the failed switch. The amber system error LED on the switch front panel blinks when beaconing is enabled. Instructions to enable beaconing are incorporated into MAP steps.

Remote Workstation Configurations

Using a standard web browser, the *HAFM* and *Product Manager* applications can be downloaded and installed on remote user workstations that are LAN-attached to the HAFM server. Operators at these workstations can manage and monitor switches controlled by the HAFM server. A maximum of nine concurrent users (including a local user) can log in to the *HAFM* application.

Each remote workstation must have access to the LAN segment on which the HAFM server is installed. Switch administrative functions are accessed through the LAN and HAFM server. The LAN interface can be:

- Part of the customer's public 10/100 Mbps LAN segment that provides access to managed switches. This switch-to-HAFM server LAN connection is part of the equipment rack installation and is required. Connection of remote workstations through the hub is optional. This type of network configuration using one Ethernet connection through the HAFM server is shown in Figure 1–6.

  This single-Ethernet connection is supported by HP, is Open View-Storage Node Manager (OV-SNM) compatible, and is the recommended configuration for a typical HP installation at a customer site. LAN security is provided by restricting password access and disabling the SNMP agent, embedded Web server interface, and command line interface (telnet access) for each managed switch.

NOTE: The Ethernet adapter in the HAFM server provides an auto-detecting 10/100 Mbps connection. Depending on speed restrictions imposed by other LAN-attached devices, the LAN segment that connects the HAFM server to manage directors and switches operates at either ten or 100 Mbps.

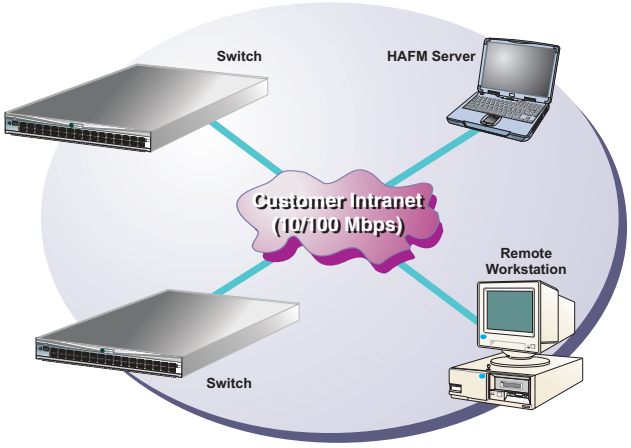


Figure 1–6: Typical Network Configuration (One Ethernet Connection)

- Part of a second HAFM server interface that connects to a customer's private intranet and allows operation of the *Product Manager* application from remote user PCs or workstations. Connection to this LAN segment is optional and depends on customer requirements. A network configuration using both Ethernet connections is shown in Figure 1–7.

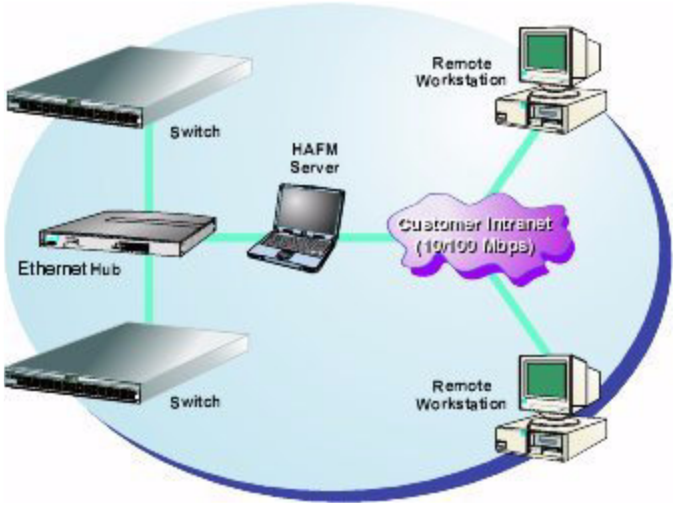


Figure 1–7: Typical Network Configuration (Two Ethernet Connections)

- Although this dual Ethernet connection is supported by HP, it is not OV-SNM compatible, requires installation of an additional PCMCIA LAN adapter card (not supplied by HP), and is not the recommended configuration for a typical new HP installation at a customer site.

Refer to the *hp StorageWorks SAN high availability planning guide* for additional information about network configurations.

CAUTION: Prior to servicing a switch or HAFM server, determine the Ethernet LAN configuration. Installation of switches and the HAFM server on a public customer intranet can complicate problem determination and fault isolation.

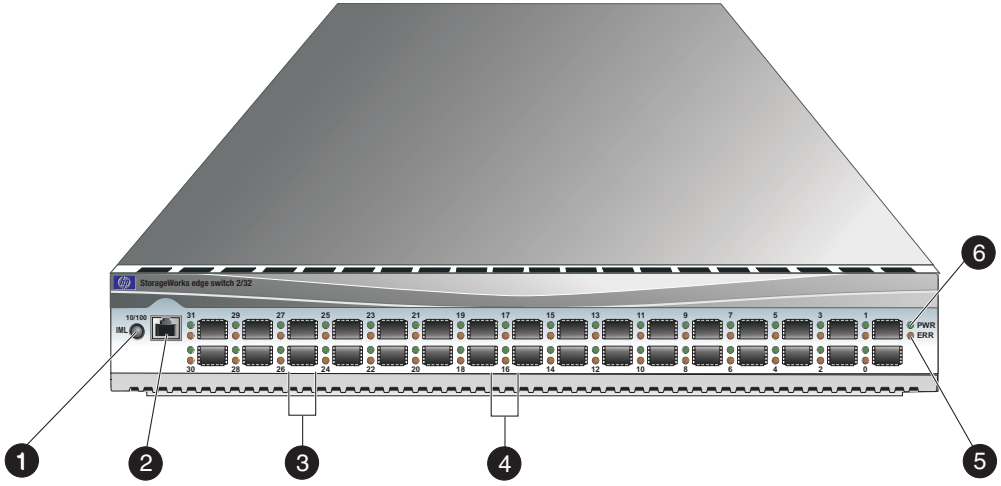
Minimum Remote Console Hardware Specifications

Client *HAFM* and *Product Manager* applications download and install to remote workstations (from the HAFM server) using a standard web browser. The applications operate on platforms that meet the following minimum system requirements:

- Desktop or notebook PC with color monitor, keyboard, and mouse, using an Intel Pentium® processor with a 400 MHz or greater clock speed, and using the Microsoft Windows® 95, Windows® 98, Windows® 2000, Windows XP, or Linux 2.2 operating system.
- UNIX workstation with color monitor, keyboard, and mouse, using a:
  - — Hewlett-Packard® HA PA-RISC® processor with a 400 MHz or greater clock speed, using the HP-UX® 11 or higher operating system.
  - — Sun® Microsystems UltraSPARC™-II processor with a 400 MHz or greater clock speed, using the SunOS™ version 5.5.1 or higher operating system, or Solaris™ version 2.5.1 or higher operating system.
  - — IBM PowerPC® microprocessor with a 400 MHz or greater clock speed, or POWER3™ microprocessor with a 400 MHz or greater clock speed, using the AIX version 4.3.3 or higher operating system.
- At least 24 MB available on the internal hard drive.
- 128 MB or greater RAM.
- Video card supporting 256 colors at 800 x 600 pixel resolution.
- Ethernet network adapter.
- Java™-enabled Internet browser, such as Microsoft® Internet Explorer (version 4.0 or later) or Netscape Navigator® (version 4.0 or later).

Field Replaceable Units

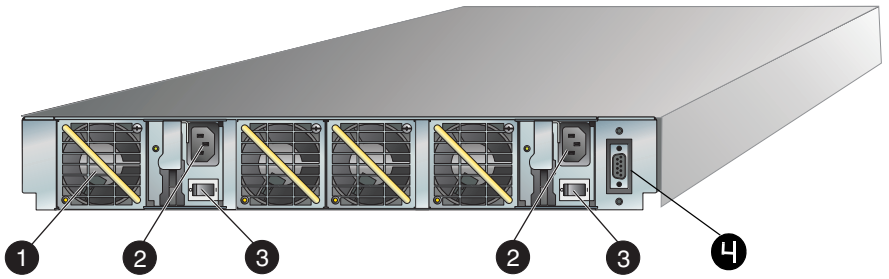
The switch provides a modular design that enables quick removal and replacement of FRUs small form factor pluggable SFP optical transceivers, power supplies, and fans. Figure 1–8 illustrates the front of the switch. The switch front panel includes:



SHR-2369

❶ Initial machine load (IML) button
❷ Ethernet LAN connector
❸ SFP fiber optic connectors
❹ Port LEDs
❺ Error LED (amber)
❻ Power LED (green)

Figure 1–8: Edge Switch 2/32 (front view)



❶ Cooling fan (4)
❷ Power supply (2)
❸ Power switches on power supplies (2)
❹ RS-232 maintenance port

Figure 1–9: Edge Switch 2/32 (rear view)

Figure 1–9 illustrates the rear of the switch. The FRUs on the rear panel include two power supplies and four individual cooling fan FRUs.

SFP Transceivers

A single-mode or multi-mode fiber-optic cable attaches to a port through a small form factor pluggable (SFP) transceiver. The SFP provides a duplex LC interface, and can be detached from the switch port for easy replacement. Two fiber-optic transceiver types are available:

- **Shortwave laser—**Shortwave laser SFPs provide short-distance connections (2 to 500 meters) through 50-micron or 62.5-micron multi-mode fiber.
- **Longwave laser—**Longwave laser SFPs provide long-distance connections (up to 10 kilometers) through 9-micron single-mode fiber.
- **Extended reach laser—**Extended reach laser SFPs provide long-distance connections (up to 35 kilometers) through 9-micron single-mode fiber.

Cooling Fans

Four fans (each a separate FRU) provide cooling for the switch power supplies and the control processor (CTP) card, as well as redundancy for continued operation if a single fan fails.

Each fan FRU can be replaced while the switch is operating.

Power Supplies

Redundant, load-sharing power supplies step down and rectify facility input power to provide 3.3 volts direct current (VDC), 5 VDC, and 12 VDC to the CTP. The power supplies also provide input filtering, overvoltage protection, and overcurrent protection. Either power supply can be replaced while the switch is operational.

Each power supply has a separate CTP connection to allow for independent AC power sources. The power supplies are input-rated at 100 to 230 volts alternating current (VAC).

Connectors and Indicators

Connectors and indicators include the:

- Initial machine load (IML) button.
- Ethernet LAN connector.
- Green power (PWR) and amber system error (ERR) LEDs.
- Green and amber status LEDs associated with FRUs.
- RS-232 maintenance port.

Initial Machine Load Button

When the IML button (Figure 1–8) is pressed and held for three seconds, the switch performs an IML that takes approximately 30 seconds and resets the:

- Microprocessor and functional logic for the CTP and loads firmware from FLASH memory.
- Ethernet LAN interface, causing the connection to the HAFM server to drop momentarily until the connection automatically recovers.
- Ports, causing all Fibre Channel connections to drop momentarily until the connections automatically recover.

An IML should only be performed if a CTP failure is indicated. Do not IML the switch unless directed to do so by a procedural step or the next level of support. As a precaution, the IML button is flush mounted to protect against accidental activation.

Ethernet LAN Connector

The front panel provides a 10/100 megabit per second (Mbps) RJ-45 twisted-pair connector (Figure 1–8) that attaches to an Ethernet LAN to provide communication with the HAFM server or an SNMP management workstation. Two green LEDs are associated with the LAN connector. When illuminated, the left LED indicates LAN operation at 10 Mbps, and the right LED indicates LAN operation at 100 Mbps.

Power and System Error LEDs

The PWR LED (Figure 1–8) illuminates when the switch is connected to facility AC power and powered on. If the LED extinguishes, a facility power source, power cord, or power distribution failure is indicated.

The ERR LED (Figure 1–8) illuminates when the switch detects an event requiring immediate operator attention, such as a FRU failure. The LED remains illuminated as long as an event is active. The LED extinguishes when the Clear System Error Light function is selected from the *Product Manager* application. The LED blinks if unit beaconing is enabled. An illuminated ERR LED (indicating a failure) takes precedence over unit beaconing.

FRU Status LEDs

Amber and green LEDs associated with switch FRUs provide status information as follows:

- **Port SFP —** Amber and green LEDs to the left of the port (Figure 1–8) illuminate, extinguish, or blink to indicate various port states (operational with active Fibre Channel traffic, operational but not communicating, beaconing, blocked, failed, inactive, or running diagnostics).
- **Fan —** An amber LED at the lower left corner of each fan (Figure 1–9) illuminates if the fan fails or rotates too slowly.
- **Power Supply —** A green LED at the upper left corner of each power supply (Figure 1–9) illuminates if the power supply is operational and receiving AC power.

Maintenance Port

The rear panel provides a 9-pin RS-232 maintenance port (Figure 1–9) that provides a connection for a local terminal or dial-in connection for a remote terminal. Although the port is typically used by authorized maintenance personnel, operations personnel can use the port to configure switch network addresses.

Software Diagnostic Features

The switch provides the following diagnostic software features that aid in fault isolation and repair of problems:

- FRUs provide on-board diagnostic and monitoring circuits that continuously report FRU status to the *HAFM* and *Product Manager* applications. These applications provide system alerts and logs that display failure and diagnostic information at the HAFM server or a remote workstation communicating with the HAFM server.
- The *HAFM Services* application that runs as a Windows 2000 service and provides an additional user interface to display operational status.
- The Embedded Web Server interface that provides Internet access to isolate problems for a single switch.
- Unsolicited SNMP trap messages that indicate operational state changes or failures can be transmitted to up to 12 authorized management workstations.
- E-mail messages or call-home reports from the HAFM server provide automatic notification of significant system events to designated support personnel or administrators.

HAFM Diagnostics

The *HAFM* application provides a Java-based GUI to manage, monitor, and isolate problems for multiple switches and multi-switch fabrics. The user interface operates locally on the HAFM server, or through an Ethernet LAN connection from a remote user workstation. The application starts automatically when the HAFM server is powered on or rebooted, and the default display is the main HAFM window, or **Product View** (Figure 1–10). If you are using a remote user workstation, see Log Into the HAFM in the *hp StorageWorks edge switch 2/32 product manager user guide*. Managed products (including switches) display as icons in the window, and a set of view tabs display at the top of the window. A status bar displays below the view area of the screen.

Figures containing HAFM and Product Manager screens in this manual are included for illustration purposed only. These illustrations may not match exactly what you see through your server or workstation. Title bars have been removed from the illustrations, and fields in the illustrations may contain different data than the screens displayed on your system.

NOTE: Icons shown in the **Product View** will vary, based on what is installed in the particular fabric being represented.

The *HAFM* application is independent from the switch or other products managed by the HAFM server. Service personnel can perform the following maintenance and diagnostic functions:

- Display the operational status for each managed product.
- Display logs that provide service and diagnostic-related information.
- Open a *Product Manager* application to monitor or fault-isolate a specific switch.
- Select the **Products** tab to view the **Hardware List View**, **Node List View**, **Port List View**, **Performance View**, and **FRU List View** and to configure and diagnose hardware problems.
- Select the **Fabrics** tab to monitor or fault-isolate multi-switch fabric problems.

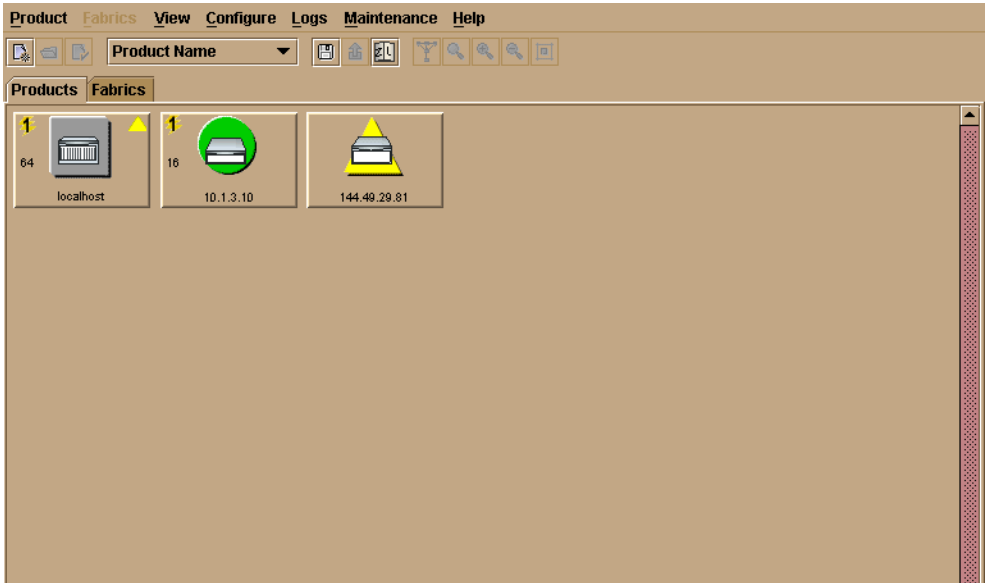


Figure 1–10: Product View

HAFM Status Symbols

A status bar at the bottom of the **Product View** displays a colored symbol that indicates the worst-case status of any managed product in the **Product View**, that fabrics are persisted in the **Fabrics View** (double-click the **Fabrics** tab), and the status of the HAFM server. Table 1–1 illustrates and explains the meaning of the status symbols. If a switch is degraded but all other managed products are fully operational, a yellow triangle displays in the status bar, and adjacent to the icon representing the degraded switch. The remaining icons have a green circle adjacent to them. By double-clicking an icon or selecting from the **View** menu, service personnel can open a specific *Product Manager* application.

A label below each icon identifies the switch by its configured name or IP address, and a colored status symbol beside each icon indicates the operational status of the switch.

Table 1–1: Status Symbols

Alert Symbol	Meaning
Green circle	**Status Bar:** All managed products are fully operational and no failures are indicated. **Next to Icon:** The switch is fully operational and no failures are indicated.
Yellow triangle	**Status Bar:** At least one managed product is operating in degraded mode. **Next to Icon:** A redundant component failed or the switch is operating in degraded mode. Service is required.
Red diamond (with yellow background)	**Status Bar:** At least one managed product is not operational. **Next to Icon:** A critical failure occurred and the switch is not operational. Immediate service is required.
Grey square	**Status Bar:** The status of at least one managed product is unknown. **Next to Icon:** The switch status is unknown because of a network connection failure between the switch and HAFM server.

Hardware View Layout and Function

Double-click a switch icon on the **Product View** to open the Product Manager for that switch. When the application opens, the default display is the **Hardware View** (Figure 1–11). The main Product Manager window (**Hardware View**) is divided into five main areas as shown in Figure 1–11 menu bar, view tabs, **Status** table, **View** panel, and status bar. Use features in these panels to configure switch operation, monitor performance, and access maintenance features.

Menu Bar

The menu bar on the Product Manager window displays tabs for the following menus:

- **Product**
- **Configure**
- **Logs**
- **Maintenance**
- **Help**

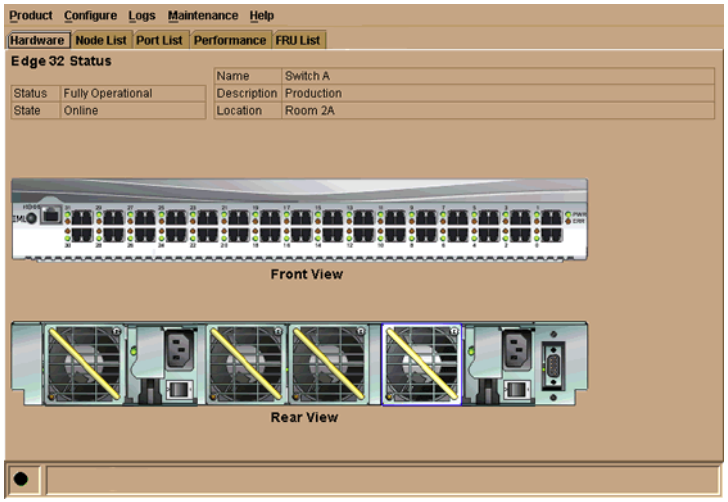
Click one of the tabs to display a list of menu options. Click an option to open a dialog box that allows you to perform configuration and maintenance tasks and view logs. If a menu option contains a check box, In the box to add a check mark and enable a function. Click a check box containing a check mark to remove the check mark and disable the function.

Product Manager Diagnostics

The *Product Manager* application provides a Java-based GUI to manage, monitor, and isolate problems for a specific switch. The application operates locally on the HAFM server, or through an Ethernet LAN connection from a remote user workstation.

Hardware View

The **Hardware View** (Figure 1–11)illustrates the following elements:



❶ Menu Bar
❷ View Tabs
❸ View Panel
❹ Status Bar

Figure 1–11: Hardware View

Service personnel can perform the following maintenance and diagnostic functions from the application:

- Observe the operational status and state, name, description, and location for the selected switch at the **Status** table at the top of the **Hardware View**.
- Observe green and amber LEDs that illuminate on graphical FRUs. These LEDs emulate LED operation on corresponding switch FRUs.
- Observe graphical FRUs that emulate the hardware configuration and operational status of the corresponding switch. Colored symbols display on graphical FRUs to represent failed or degraded status. The colors and shapes are consistent with other status displays.
- Select a view tab to perform maintenance functions or display logs that provide service and diagnostic-related information.
- Select graphical FRUs with the mouse to display maintenance-related dialog boxes or perform maintenance functions.

Status Table

The switch **Status** table displays the selected switch operational status, operational state, port state, name, description, and location. The **Status** field shows one of the following:

- **Fully Operational —** all switch FRUs and ports are fully operational, and no failures are indicated.
- **Redundant Failure —** a redundant FRU failed (power supply or fan FRU) and the switch is operational. In addition to the text message, the **Status** and **State** fields change to a yellow background (refer to Figure 1–12, Hardware View).
- **Minor Failure —** a failure occurred that decreased the operational capability of the switch (port SFP failure), but has not affected normal switching operations. In addition to the text message, the **Status** and **State** fields change to a yellow background (refer to Figure 1–12).
- **Not Operational —** the switch failed, is not operational, and requires immediate service. In addition to the text message, the **Status** and **State** fields change to a yellow background (refer to Figure 1–12).
- **No Link —** if the switch-to-HAFM server link is down, **No Link** displays in the **Status** field, the **Status** and **State** fields change to a yellow background, the **Name**, **Description**, and **Location** fields do not display, and the **State** field changes to a **Reason** field with a brief description of the link loss condition. For a description of link loss conditions, refer to MAP 0400: Loss of Console Communication on page 2–39.

The **State** field shows one of the following:

- `Online` **—** when the switch is set online, an unblocked port and all unbypassed ports are awaiting device login and are able to attach to a device. This state is configured through the **Set Online State** dialog box or following an IML.
- `Offline` **—** when the switch is set offline, all ports are offline and cannot accept a login from an attached device that requires a switch connection. This state is configured through the **Set Online State** dialog box.
- `Coming online` **—** this is a transitional state that occurs just prior to the switch going online. Unless a problem occurs, this state displays only briefly. The switch automatically transitions through this state after a power-up or reset procedure.
- `Going offline` **—** this is a transitional state that occurs just prior to the switch going offline. Unless a problem occurs, this state displays only briefly.

LED Emulation

At the **Hardware View** for the selected switch, simulated LEDs illuminate on FRUs and adjacent to port SFPs to emulate the operation of LEDs on the corresponding hardware. Simulated PWR and ERR LEDs also illuminate to emulate the operation of LEDs on the corresponding switch front panel. For an explanation of LED operation, refer to FRU Status LEDs.

Product Manager Status Symbols

A status bar at the bottom of the window displays a colored symbol (green circle, yellow triangle, red diamond with yellow background, or grey square) that indicates the worst-case status of the selected switch. The meaning of the status symbol is consistent with the icon explanations in Table 1–1.

As an example, for a single SFP, fan, or power supply failure, a blinking red and yellow diamond displays at the FRU illustration in the **Hardware View**. However, the status bar displays a yellow triangle to indicate degraded operation. If a blinking red and yellow diamond displays over multiple FRUs, the status bar displays a red and yellow diamond, indicating a critical failure and the switch is not operational.

The following colored symbols overlay graphical FRUs to represent failed or degraded status for the corresponding switch FRU.

- **Failed FRU indicator —** a blinking (color reversing) red and yellow diamond overlaying a FRU indicates the FRU failed and immediate service is required.
- **Attention indicator —** a yellow triangle overlaying the top of a port SFP indicates the port is in a nonstandard mode or configuration, but did not actually fail. The indicator displays for any port having a state other than online, failed, blocked, bypassed, or loss of light. The indicator also displays to indicate a link incident (LIN) alert or a segmented port.

View Tabs

Click one of the view tabs across the top of the Product Manager window to display the following views in the **View** panel.

- **Hardware**
- **Node List**
- **Port List**
- **Performance**
- **FRU List**

View Panel

Views, selected from the view tabs, display in the **View** panel.

Hardware View

The **Hardware View** is the default view that displays in the **View** panel when you open the switch Product Manager. To return to this view from another view, click the **Hardware View** tab. Refer to Figure 1–12 for an example of this view.

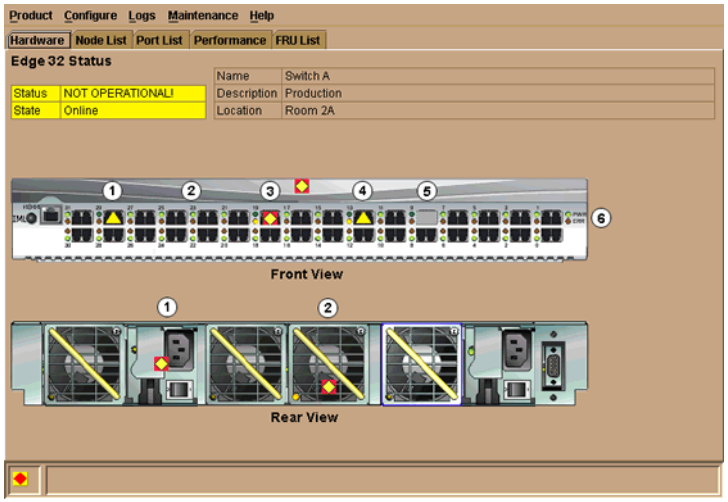

Product Configure Logs Maintenance Help
Hardware Node List Port List Performance FRU List
Edge 32 Status
Name Switch A
Status NOT OPERATIONAL! Description Production
State Online Location Room 2A
1 2 3 4 5 6
Front View
1 2
Rear View

Figure 1–12: Hardware View

In the **Hardware View**, colored indicators reflect the status of actual LEDs on the switch FRUs. The status bar displays a symbol to represent the most degraded status currently reported by any of the switch FRUs. For example, for a port failure, indicated by a blinking red and yellow diamond on a port, a yellow triangle displays on the status bar to indicate a degraded condition. However, if a blinking red and yellow diamond displays over both power supplies, the status bar displays a blinking red and yellow diamond, which indicates a failure requiring immediate attention. For an explanation of the different status symbols and the reasons they display in the **Hardware View** or **Port List View**, refer to Table 1–1.

Switch Menu

Double-click the switch graphic away from a FRU to display the **Switch Properties** dialog box. Right-click a hardware graphic away from a FRU to display the following options:

- Switch Properties
- Enable Unit Beaconing
- Clear System Error Light
- IPL Switch
- Set Switch Date and Time
- Set Switch Online State

Port Menu

Double-click a port to display the **Port Properties** dialog box. Right-click a port to display the following options:

- **Port Properties**
- **Node Properties**
- **Port Technology**
- **Block Port**
- **Enable Beaconing**
- **Channel Wrap (S/390 mode only)**
- **Swap Ports (S/390 mode only)**
- **Port Diagnostics**
- **Clear Link Incident Alert(s)**
- **Reset Port**
- **Port Binding**
- **Clear Threshold Alert(s)**

Note that these same options are available when you click a port on the **Hardware View** and select the **Port** secondary menu from the **Product** menu on the menu bar.

NOTE: For *Node Properties*, if a node is not logged in a message box displays indicating that node information is not available.

Port List View

Select the **Port List View** tab. A table listing the port number, port name, port address (S/390 mode only), the block/unblock configuration, operating state, port type, operating speed, and alert condition displays in the **View** panel. Figure 1–13 shows an example of the **Port List View**.

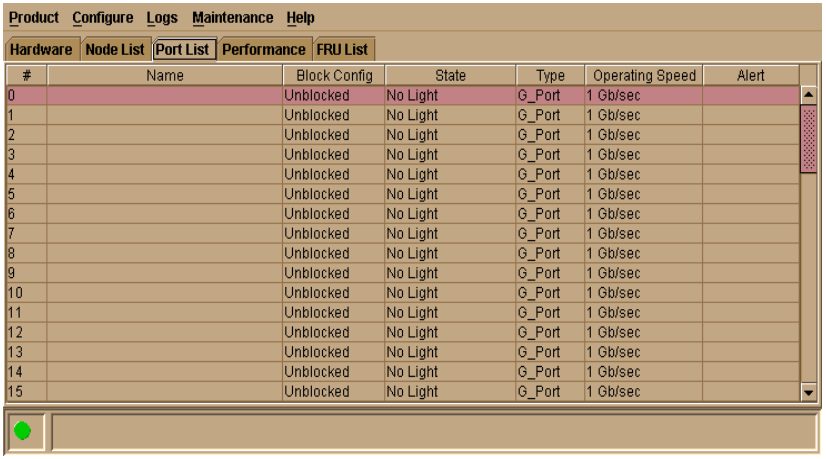

Product Configure Logs Maintenance Help
Hardware Node List Port List Performance FRU List
Name Block Config State Type Operating Speed Alert
0 Unblocked No Light G_Port 1 Gb/sec
1 Unblocked No Light G_Port 1 Gb/sec
2 Unblocked No Light G_Port 1 Gb/sec
3 Unblocked No Light G_Port 1 Gb/sec
4 Unblocked No Light G_Port 1 Gb/sec
5 Unblocked No Light G_Port 1 Gb/sec
6 Unblocked No Light G_Port 1 Gb/sec
7 Unblocked No Light G_Port 1 Gb/sec
8 Unblocked No Light G_Port 1 Gb/sec
9 Unblocked No Light G_Port 1 Gb/sec
10 Unblocked No Light G_Port 1 Gb/sec
11 Unblocked No Light G_Port 1 Gb/sec
12 Unblocked No Light G_Port 1 Gb/sec
13 Unblocked No Light G_Port 1 Gb/sec
14 Unblocked No Light G_Port 1 Gb/sec
15 Unblocked No Light G_Port 1 Gb/sec

Figure 1–13: Port List View

The **Port List View** displays information about all ports installed in the switch. All data is dynamic and updates automatically. Double-click any row in this view to display the **Port Properties** dialog box for the port.

Right-click a port row to display the same menu options that display when you right-click a port in the **Hardware View** or a port's bar graph in the **Performance View**. These include:

- **Port Properties**
- **Node Properties**
- **Port Technology**
- **Block Port**
- **Enable Beaconing**
- **Port Diagnostics**
- **Channel Wrap (S/390 mode only)**

- **Swap Ports (S/390 mode only)**
- **Clear Link Incident Alert(s)**
- **Reset Port**
- **Port Binding**
- **Clear Threshold Alert(s)**

Note that these options are also available when you click a port row and select the **Port** secondary menu from the **Product** menu on the menu bar.

FRU List View

Select the **FRU List View** tab. A table with information about each of the FRUs installed in the switch displays in the **View** panel. All data is dynamic and updates automatically. Figure 1–14 shows an example of the **FRU List View**.

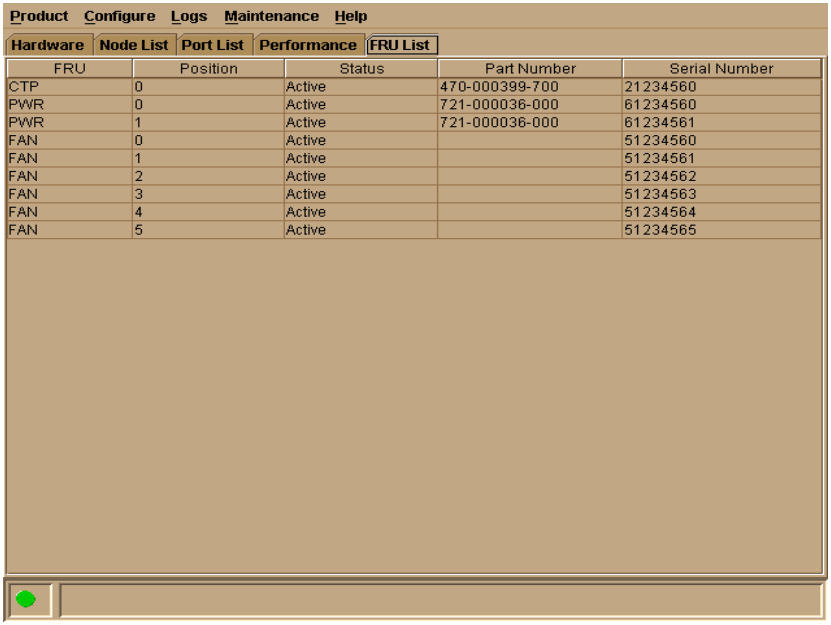


Figure 1–14: FRU List View

Node List View

Select **Node List** from view tabs. Figure 1–15 on page 1-32 shows an example of the **Node List View**. This view displays a table with information about all node attachments or N_Ports that have logged into existing F_Ports on the switch. Only N_Ports display in the **Node List View** after nodes have logged in to the fabric. The columns that display in the table include: port number where the node is attached, the port's address (S/390 mode only), node type, WWN of the attached node (device), and BB_Credit used by the attached node.

Double-click a port row to highlight it and display the **Node Properties** dialog box for that port.

Right-click a port row to display the following menu options:

- **Node Properties:** Displays the **Node Properties** dialog box.
- **Port Properties:** Displays the **Port Properties** dialog box.
- **Define Nickname:** Displays the **Define Nickname** dialog box, where you can define a nickname to display for the attached device instead of the device's 8-byte WWN.
- **Display options:** Allows you to display attached devices listed under the **Port WWN** column in the **Node List View** by the device's nickname configured through the **Define Nickname** menu option or the device's WWN.

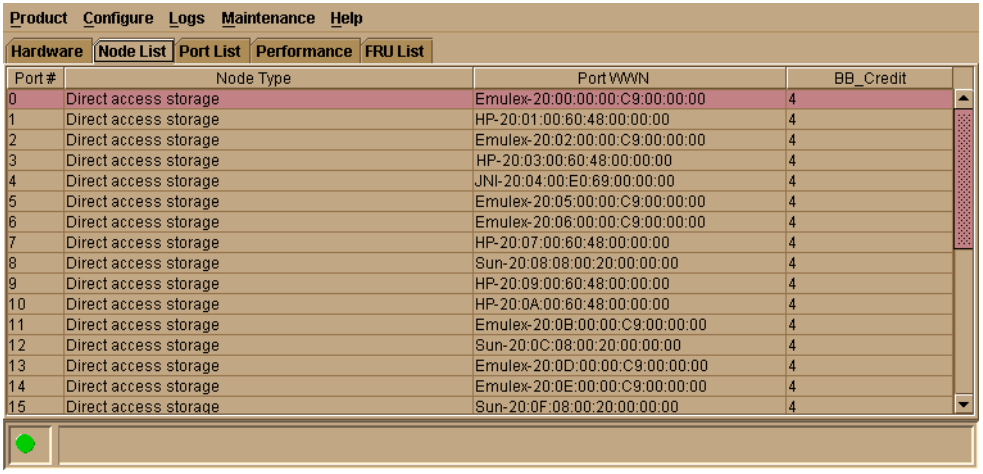

Product Configure Logs Maintenance Help
Hardware Node List Port List Performance FRU List
Port # Node Type Port WWN BB_Credit
0 Direct access storage Emulex-20:00:00:00:C9:00:00:00 4
1 Direct access storage HP-20:01:00:60:48:00:00:00 4
2 Direct access storage Emulex-20:02:00:00:C9:00:00:00 4
3 Direct access storage HP-20:03:00:60:48:00:00:00 4
4 Direct access storage JNI-20:04:00:E0:69:00:00:00 4
5 Direct access storage Emulex-20:05:00:00:C9:00:00:00 4
6 Direct access storage Emulex-20:06:00:00:C9:00:00:00 4
7 Direct access storage HP-20:07:00:60:48:00:00:00 4
8 Direct access storage Sun-20:08:08:00:20:00:00:00 4
9 Direct access storage HP-20:09:00:60:48:00:00:00 4
10 Direct access storage HP-20:0A:00:60:48:00:00:00 4
11 Direct access storage Emulex-20:0B:00:00:C9:00:00:00 4
12 Direct access storage Sun-20:0C:08:00:20:00:00:00 4
13 Direct access storage Emulex-20:0D:00:00:C9:00:00:00 4
14 Direct access storage Emulex-20:0E:00:00:C9:00:00:00 4
15 Direct access storage Sun-20:0F:08:00:20:00:00:00 4

Figure 1–15: Node List View

Note that these options are also available when you click a port row, then select the **Port** secondary menu from the **Product** tab on the menu bar.

Performance View

Select the **Performance View** tab from the menu. Figure 1–16 shows an example of the **Performance View**. This view provides a graphical display of performance for all 32 ports. The top portion of the **Performance View** displays bar graphs that show the level of transmit/receive activity for each port. This information updates every five seconds. Each bar graph also shows the percentage link utilization for the port. A red arrow marks the highest utilization level reached since the **Performance View** was opened. If the system detects activity on a port, it represents minimal activity with at least one bar.

When an end device (node) is logged into a port, moving the cursor over the port's bar graph in the **Performance View** highlights the graph and displays a message with the world-wide name of the connected node. If the connected node has more than one port, this is the world-wide name of the specific port on the node. When a port is functioning as an expansion port (E_Port), the message is `E_Port`. When a port is not logged into an end-device (not functioning as an F_Port) or to another switch (not functioning as an E_Port), the message is the port's current online state.

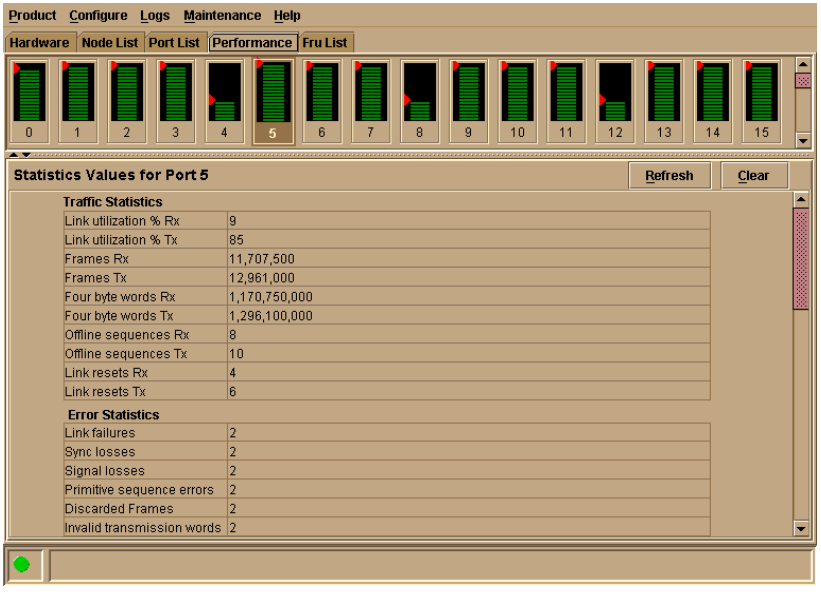

Product Configure Logs Maintenance Help
Hardware Node List Port List Performance Fru List
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
Statistics Values for Port 5
Refresh
Clear
Traffic Statistics
Link utilization % Rx 9
Link utilization % Tx 85
Frames Rx 11,707,500
Frames Tx 12,961,000
Four byte words Rx 1,170,750,000
Four byte words Tx 1,296,100,000
Offline sequences Rx 8
Offline sequences Tx 10
Link resets Rx 4
Link resets Tx 6
Error Statistics
Link failures 2
Sync losses 2
Signal losses 2
Primitive sequence errors 2
Discarded Frames 2
Invalid transmission words 2

Figure 1–16: Performance View

Right-click a bar graph to display a menu of port-related actions. The options available on this menu are the same as those that are available when you right-click a port in the **Hardware View** or right-click a row in the **Port List View**. These include:

- **Port Properties**
- **Node Properties**
- **Port Technology**
- **Block Port**
- **Enable Beaconing**
- **Port Diagnostics**
- **Channel Wrap** (S/390 mode only)
- **Swap Ports** (S/390 mode only)
- **Clear Link Incident Alert(s)**
- **Reset Port**
- **Port Binding**
- **Clear Threshold Alert(s)**

Note that these same options are also available when you click a port's graph, then select the **Port** secondary menu from the **Product** menu on the menu bar.

The bottom portion of the **Performance View** displays cumulative statistical information for the port selected in the bar graph. Click the **Refresh** button to update the data with current data from the port.

Click the **Clear** button to clear all of the counters to zero for the selected port and to place an entry in the audit log indicating that statistics for the port have been cleared.

NOTE: Clearing the counters clears the statistics for all users.

Status Bar

The status bar is located along the bottom of the Product Manager window. This includes a symbol that displays at the left side of the bar and messages that display in the panel to the right of the symbol. The symbol indicates the current operating status of the switch and the messages display to provide more description of menu options as you move the cursor over the options under menu bar menus. Refer to Table 1–2 for the meaning of these status symbols and of the corresponding alert text that displays in the Edge-32 **Status** table at the top of the **Hardware View** in the **View** panel.

If a gray square displays in the status bar (no Ethernet connection), a reason for the status displays in the **Status** table at the top of the **Hardware** View.

Table 1–2: Operating Status — Status Bar and Switch Status Table

Symbol	Status Bar	Switch Status Table Text	Meaning
	Green Circle	Fully Operational	All components and installed ports are operational; no failures.

Table 1–2: Operating Status — Status Bar and Switch Status Table (Continued)

Symbol	Status Bar	Switch Status Table Text	Meaning
	Yellow Triangle	Redundant Failure	A redundant component has failed, such as a power supply, and the backup component has taken over operation.
		Minor Failure	A failure occurred which has decreased the switch operational ability. Normal switching operations are not affected. One or more ports failed, but at least one port is still operational. A fan has failed or is not rotating sufficiently.
	Blinking Red and Yellow Diamond	NOT OPERATIONAL	A critical failure prevents the switch from performing fundamental switching operations. • All fans failed. • All installed ports failed. • Both power supplies failed.
	Gray Square	Never Connected Link Timeout Protocol Mismatch Duplicate Session Unknown Network Address Incorrect Product Type	Switch status is unknown. This occurs if the Ethernet network connection between the HAFM server and the switch cannot be established or if the CTP fails.

Messages display to the right of the status symbol as you move the cursor over options under the menu bar menus. These messages provide additional details about tasks that you can perform through the menu option.

Fabrics View

Access the **Fabrics View** by clicking the **Fabrics** tab on the *HAFM* application window. The left panel of this view is the **Fabric Tree**, which is the expandable list of fabrics, products in fabrics, and nodes connected to products. The view area for the tab is to the right of the Fabric Tree.

Click the **Topology** and **Zone Set** tabs at the bottom of the view area to change the views. The **Topology** tab (default) is illustrated in Figure 1–17 and the **Zone Sets** tab is illustrated in Figure 1–18.

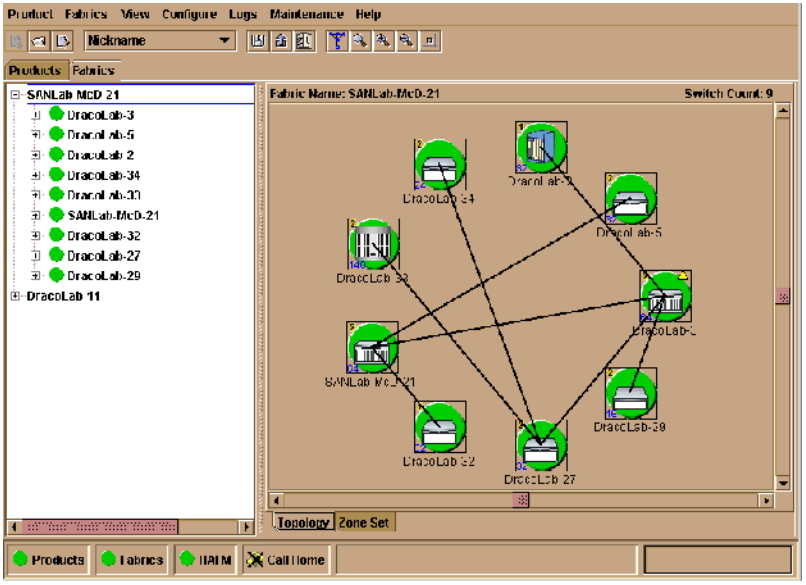


Figure 1–17: Fabrics View — Topology Tab

Topology Tab

The view area of the **Topology** tab provides details on all fabrics known to the HAFM server and *HAFM* application. This area displays product icons like those in the **Products** view, each representing switches and directors in fabrics that you select from a Fabric Tree on left panel of the view. Interswitch links (ISLs) display between the product icons as black lines. Fabrics are initially listed in the Fabric Tree by the world wide name (WWN) of the fabric's principal switch, but if the fabric is "persisted," they could have various names configured by the user. The selected fabric's name displays above the icons at the top of the tab.

Zone Set Tab

This tab displays the currently active zone set for fabrics that you select from the left side of the view. The zones and zone members that make up the zone set display in a scrollable tree structure below the name of the active zone set. Menu options available in this tab allow you to quickly determine fabric zoning structure (zone sets, zones, and zone members), determine logged in and logged out zone members, save active zones under another name, determine the default zone members, deactivate/activate zone sets, and change the default zone.

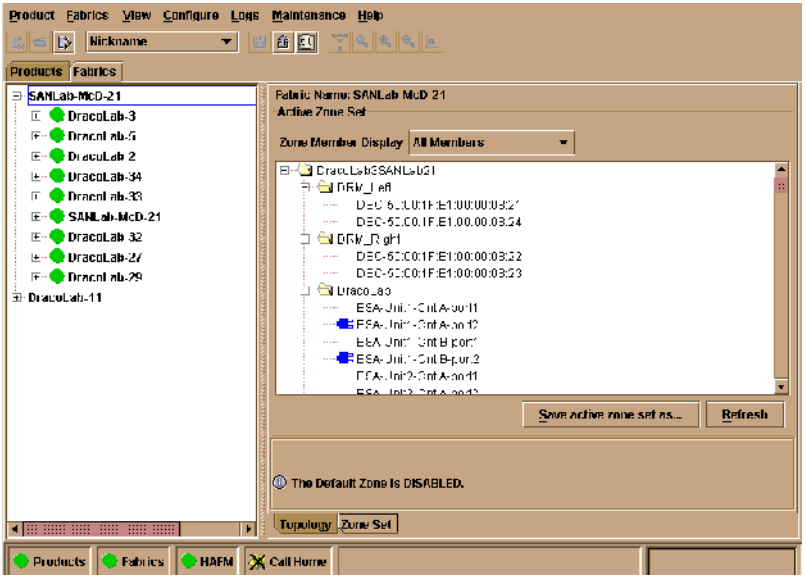


Figure 1–18: Fabrics View — Zone Sets Tab

HAFM Services Application

The HP StorageWorks *High Availability Fabric Manager* (*HAFM*) *Services* application provides both a central control point and server-side functionality (in a client-server environment) for all HP managed products. The application runs as a Windows 2000 service and starts automatically when the HAFM server is powered on.

The user interface consists of the HAFM Services window (Figure 1–19), which provides *HAFM* application status and diagnostic information. The HAFM Services window consists of:

- An event table that displays HAFM Services events that occurred since the *HAFM* application was started.
- A status line at the bottom of the panel that provides a status indicator and message area.

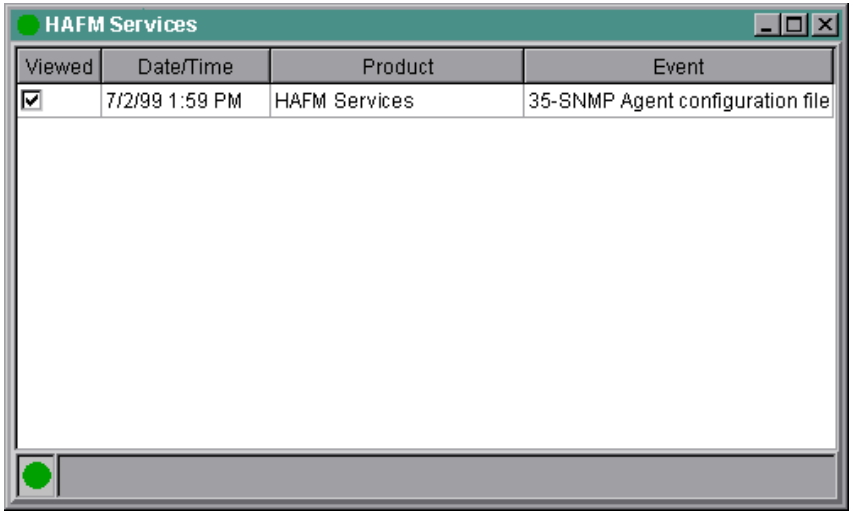


Figure 1–19: HAFM Services Window

Event Table

The event table displays the last ten events that occurred since the *HAFM* application was started. Events that occurred during a prior instance of the application do not display. If a new event occurs while ten events display, the oldest event is discarded. A deeper event history is maintained in the form of a log file viewed through the *HAFM* application.

The events are internal error conditions detected by the *HAFM* application, and are not related to product-specific events reported by a switch. Events typically relate to HAFM audit log and file corruption, invalid product definition and firmware files, missing product services class, or missing version information.

The event table contains the following columns:

- **Viewed —** this column provides a check box associated with each event. Each check box allows service personnel to mark an event as viewed (acknowledged with appropriate action taken).

- **Date/Time —** the date and time the event was reported to the HAFM server.
- **Product —** the product associated with the event. Some events are associated with the *HAFM* application, while others are associated with a specific instance of the *Product Manager* application. In the latter case, the switch and configured name (or IP address) associated with the instance are displayed.
- **Event —** the numeric event code and a brief description of the event.

Status Line

The status line provides a status indicator and message area. HAFM status symbols are explained in Table 1–3.

The ***HAFM* application** icon (upper left corner of the window) is dynamic and matches the status indicator. This feature allows users and service personnel to observe the status when the application is minimized to the Windows 2000 task bar.

The message area briefly displays messages during *HAFM* application startup to indicate the progress of startup activities.

Table 1–3: HAFM Services Status Symbols

Alert Symbol	Meaning
Blank	The status indicator is blank during *HAFM* application initialization.
Green circle	All events are viewed (acknowledged with appropriate action taken).
Yellow triangle	One or more nonfatal events have not been viewed.
Red diamond (with yellow background)	A fatal error occurred.

Embedded Web Server Diagnostics

If the HP StorageWorks High Availability Fabric Manager (HAFM) server access is not available, the Embedded Web Server interface provides a GUI accessed through the Internet (locally or remotely) to manage, monitor, and isolate problems for a single switch. This interface is available with switch firmware Version 1.2 (or later) installed, and does not replace nor offer the full management capability of the *HAFM* and switch *Product Manager* applications.

The Embedded Web Server interface can be opened from a standard web browser running Netscape Navigator® 4.6 or higher or Microsoft Internet Explorer 4.0 or higher. At the browser, enter the IP address of the switch as the Internet uniform resource locator (URL). When prompted at a login screen, enter a user name and password. When the interface opens, the default display is the **View** panel. Service personnel can perform the monitoring, configuration, maintenance and diagnostic functions as follows:

- **View panel —** quickly inspect and determine the operational status of the switch, and inspect switch properties and operating parameters, FRU properties, and Fibre Channel port properties.
- **Configure panel —** configure or change:
  - — Switch ports.

  - — Switch identification, date and time, operating parameters, and network addresses.
  - — SNMP trap message recipients.
  - — User passwords.
- **Monitor panel —** inspect and monitor:
  - — Fibre Channel ports and port performance statistics.
  - — The active zone set.
  - — Event log entries, and clear the IML LED at the front panel.
  - — Information about attached devices (nodes).
- **Operations panel —** perform the following operations and maintenance tasks:
  - — Enable port beaconing and perform port diagnostics (internal and external loopback tests).
  - — Reset Fibre Channel ports.
  - — Set the switch online state.
  - — Upgrade switch firmware.

General tasks performed through the web server interface are similar in form and function to tasks performed through the *HAFM* and *Product Manager* applications, and are therefore not documented in this publication. For task information and descriptions, open the online user documentation (Help selection) that supports the interface.

This publication provides instructions for switch installation and fault isolation using the Embedded Web Server interface. Refer to the *hp StorageWorks edge switch 2/32 installation guide* for installation and configuration tasks. Refer to Chapter 2 for fault isolation tasks.

SNMP Trap Message Support

Unsolicited SNMP trap messages that indicate switch operational state changes or failure conditions can be customer-configured to be transmitted to up to 12 management workstations. If installed on a dedicated Ethernet LAN, the workstations communicate directly with each switch. If installed on a customer intranet, the workstations communicate with switches through the HAFM server.

SNMP data and trap messages are defined in the Fibre Channel FE-MIB definition, a subset of the TCP/IP MIB-II definition (RFC1213), and a custom, switch-specific MIB. Customers can install these MIBs (in standard ASN.1 format) on any SNMP management workstation.

Although SNMP trap messages are typically transmitted to customer personnel only, the messages may be provided to service personnel as initial notification of a switch problem or as information included in the fault isolation process. Generic SNMP traps include:

- **coldStart —** reports that the SNMP agent is reinitializing due to a switch reset.
- **warmStart —** reports that the SNMP agent is reinitializing due to a switch IPL.
- **authorizationFailure —** reports access by an unauthorized SNMP manager. This trap is configurable, and is disabled by default.

Switch-specific SNMP traps specified in the custom MIB include Fibre Channel port operational state changes and FRU operational state changes.

If authorized through the **Configure SNMP** dialog box in the *Product Manager* application, users at SNMP management workstations can modify MIB variables. Switch modifications performed through SNMP management work stations are recorded in the associated switch audit log and are available through the *Product Manager* application.

For additional information, refer to the *hp StorageWorks SNMP reference guide for directors and edge switches*.

E-Mail and Call-Home Support

If e-mail notification and call-home support are configured for the switch as part of the customer support process, service personnel may be:

- Notified of a switch problem by e-mail message, either directly or through a system administrator at the customer site or call center.
- Assigned a service call from call center personnel upon receipt and confirmation of a switch call-home event.

Tools and Test Equipment

This section describes tools and test equipment that may be required to install, test, service, and verify operation of the switch and attached HAFM server.

Tools Supplied with the Switch

The following tools are supplied with the switch. Use of the tools may be required to perform one or more installation, test, service, or verification tasks. These tools are supplied with the switch or must be supplied by service personnel.

- Fiber-optic loopback plug **—** An SFP multi-mode (shortwave laser) or single-mode (longwave laser) loopback plug is required to perform port loopback diagnostic tests. One loopback plug is shipped with the switch, depending on the type of port transceivers installed. Both plugs are shipped if shortwave laser and longwave laser transceivers are installed. The plug is shown in Figure 1–20.

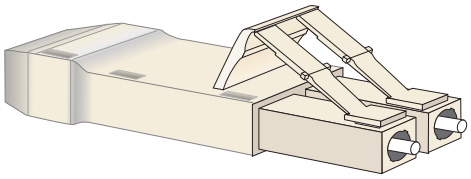


Figure 1–20: Multi-mode and Single-mode Loopback Plugs

- **Fiber-optic protective plug —** For safety and port transceiver protection, fiber-optic protective plugs must be inserted in all port SFPs without fiber-optic cables attached. The switch is shipped with protective plugs installed in all ports. A protective plug is shown in Figure 1–21.

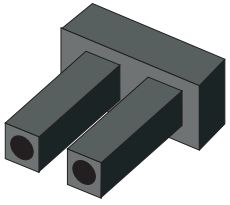


Figure 1–21: Fiber-Optic Protective Plug

- **Null modem cable —** An asynchronous RS-232 null modem cable is required to configure switch network addresses and acquire event log information through the maintenance port. The cable has nine conductors and DB-9 male and female connectors. A null modem cable is not a standard (straight-through) RS-232 cable. Refer to Figure 1–22.

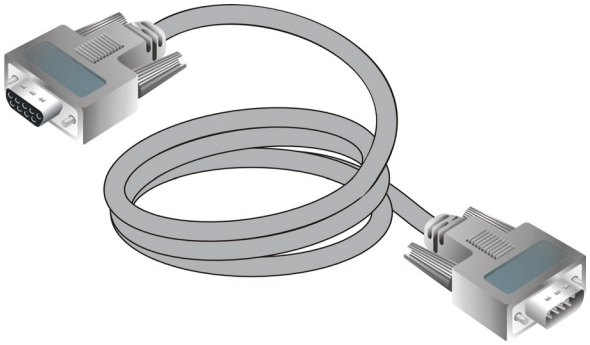


Figure 1–22: Null Modem Cable

Tools Supplied by Service Personnel

The following tools are expected to be supplied by service personnel performing switch installation and maintenance actions. Use of the tools may be required to perform one or more installation, test, service, or verification tasks.

- **Scissors or pocket knife —** A sharp cutting edge (scissors or knife blade) may be required to cut the protective strapping when unpacking the switch, HAFM server, Ethernet hub, or replacement FRUs.
- **Standard flat-tip and cross-tip (Phillips) screwdrivers —** Screwdrivers are required to remove, replace, adjust or tighten various connector or chassis components, and to remove and replace power supplies.
- **Maintenance terminal (desktop or notebook PC) —** the PC is required to configure switch network addresses and acquire event log information through the maintenance port. The PC must have:
  - The Microsoft Windows 98, Windows 2000, or Windows Millennium Edition operating system installed.
  - RS-232 serial communication software (such as ProComm Plus™ or HyperTerminal) installed. HyperTerminal is provided with Windows operating systems.
- **Fiber-optic cleaning kit —** The kit contains tools and instructions to clean fiber-optic cable, connectors, loopback plugs, and protective plugs.

2

Diagnostics

This chapter describes diagnostic procedures used by service representatives to isolate HP StorageWorks Edge Switch 2/32 problems or failures to the field-replaceable unit (FRU) level. The chapter specifically describes how to perform maintenance analysis procedures (MAPs).

Maintenance Analysis Procedures

The MAPs provide fault isolation and related service procedures. They are step-by-step procedures that prompt service personnel for information and describe a maintenance action. They provide information to interpret system events, isolate a switch failure to a single FRU, remove and replace the failed FRU, and verify switch operation.

Factory Defaults

Table 2–1 lists the defaults for the passwords, and IP, subnet, and gateway addresses.

Table 2–1: Factory-Set Defaults

Item	Default
Customer password	password
Maintenance password	level-2
IP address	10.1.1.10
Subnet mask	255.0.0.0
Gateway address	0.0.0.0

Quick Start

Table 2–2 lists the MAPs in this chapter. Fault isolation normally begins at "MAP 0000: Start MAP" on page 2-7.

However, Table 2–3 lists the event codes and the corresponding MAPs. It is a quick start, if an event code is readily available.

Table 2–2: MAP Summary

MAP	Page
MAP 0000: Start MAP	page 2–7
MAP 0100: Power Distribution Analysis	page 2–26
MAP 0200: POST, Reset, or IPL Failure Analysis	page 2–32
MAP 0300: Console Application Problem Determination	page 2–33
MAP 0400: Loss of Console Communication	page 2–39
MAP 0500: Fan and CTP Failure Analysis	page 2–58
MAP 0600: Port Failure and Link Incident Analysis	page 2–63
MAP 0700: Fabric, ISL, and Segmented Port Problem Determination	page 2–79
MAP 0800: Console PC Problem Determination	page 2–90

Table 2–3: Event Codes versus Maintenance Action

Event Code	Explanation	Action
001	System power-down.	Power on switch.
011	Login server database invalid.	Go to MAP 0700.
021	Name server database invalid.	Go to MAP 0700.
031	SNMP request received from unauthorized community.	Add community name.
051	Management server database invalid.	Go to MAP 0700.
052	Management server internal error.	Go to MAP 0700.
061	Fabric controller database invalid.	Go to MAP 0700.

Table 2–3: Event Codes versus Maintenance Action (Continued)

Event Code	Explanation	Action
062	Maximum interswitch hop count exceeded.	Go to MAP 0700.
070	E_Port is segmented.	Go to MAP 0700.
071	Switch is isolated.	Go to MAP 0700.
072	E_Port connected to an unsupported switch.	Go to MAP 0700.
080	Unauthorized world wide name	Go to MAP 0600
200	Power supply ac voltage failure.	Go to MAP 0100.
201	Power supply DC voltage failure.	Go to MAP 0100.
202	Power supply thermal failure.	Go to MAP 0100.
203	Power supply ac voltage recovery.	No action required.
204	Power supply DC voltage recovery.	No action required.
206	Power supply removed.	Replace FRU.
207	Power supply installed.	No action required.
208	Power supply false shutdown.	Go to MAP 0100.
300	First cooling fan failed.	Go to MAP 0500.
301	Second cooling fan failed.	Go to MAP 0500.
302	Third cooling fan failed.	Go to MAP 0500.
303	Fourth cooling fan failed.	Go to MAP 0500.

Table 2–3: Event Codes versus Maintenance Action (Continued)

Event Code	Explanation	Action
304	Fifth cooling fan failed (does not apply to Edge Switch 32).	Go to MAP 0500.
305	Sixth cooling fan failed (does not apply to Edge Switch 32).	Go to MAP 0500.
306	First cooling fan in fan FRU assembly failed. (does not apply to Edge Switch 32)	Go to MAP 0500.
307	Second cooling fan in fan FRU assembly failed. (does not apply to Edge Switch 32)	Go to MAP 0500.
310	First cooling fan recovered.	No action required.
311	Second cooling fan recovered.	No action required.
312	Third cooling fan recovered.	No action required.
313	Fourth cooling fan recovered.	No action required.
314	Fifth cooling fan recovered (does not apply to Edge Switch 32).	No action required.
315	Sixth cooling fan recovered (does not apply to Edge Switch 32).	No action required
316	First cooling fan in fan FRU assembly recovered. (does not apply to Edge Switch 32)	No action required.
317	Second cooling fan in fan FRU assembly recovered. (does not apply to Edge Switch 32)	No action required.
400	Power-up diagnostic failure.	Go to MAP 0200.
410	CTP reset.	No action required.

Table 2–3: Event Codes versus Maintenance Action (Continued)

Event Code	Explanation	Action
411	Firmware fault occurred.	Go to MAP 0200.
421	Firmware download complete.	No action required.
423	CTP firmware download initiated.	No action required.
430	Excessive Ethernet transmit errors.	Go to MAP 0400.
431	Excessive Ethernet receive errors.	Go to MAP 0400.
432	Ethernet adapter reset.	Go to MAP 0400.
433	Non-recoverable Ethernet fault.	Go to MAP 0400.
440	Embedded port hardware failure.	Go to MAP 0600.
502	Port module anomaly detected.	No action required.
504	Port module failure — error threshold exceeded.	Go to MAP 0600.
505	Port module revision not supported.	No action required.
506	Fibre Channel port failure.	Go to MAP 0600.
507	Loopback diagnostics port failure.	Go to MAP 0600.
508	Fibre Channel port anomaly detected.	Go to MAP 0600.
510	SFP hot-insertion initiated.	No action required.
512	SFP nonfatal error.	Go to MAP 0600.

Table 2–3: Event Codes versus Maintenance Action (Continued)

Event Code	Explanation	Action
513	SFP hot-removal completed.	No action required.
514	SFP failure.	Go to MAP 0600.
581	Implicit incident.	Go to MAP 0600.
582	Bit-error threshold exceeded.	Go to MAP 0600.
583	Loss of signal or loss of synchronization.	Go to MAP 0600.
584	Not operational primitive sequence (NOS) received.	Go to MAP 0600.
585	Primitive sequence timeout.	Go to MAP 0600.
586	Invalid primitive sequence received for link state.	Go to MAP 0600.
602	SBAR anomaly detected.	No action required.
604	SBAR failure.	Go to MAP 0600.
605	SBAR revision not supported.	Go to MAP 0600.
800	High-temperature warning (port module thermal sensor).	Go to MAP 0500.
801	Critically hot temperature warning (port module thermal sensor).	Go to MAP 0500.
802	Port module shutdown due to thermal violations.	Go to MAP 0500.
805	High-temperature warning (SBAR thermal sensor).	Go to MAP 0500.
806	Critically hot temperature warning (SBAR thermal sensor).	Go to MAP 0500.

Table 2–3: Event Codes versus Maintenance Action (Continued)

Event Code	Explanation	Action
807	SBAR shutdown due to thermal violations.	Go to MAP 0500.
810	High-temperature warning (CTP thermal sensor).	Go to MAP 0500.
811	Critically hot temperature warning (CTP thermal sensor).	Go to MAP 0500.
812	CTP shutdown due to thermal violations.	Go to MAP 0500.
850	System shutdown due to CTP thermal violations.	Go to MAP 0500.

MAP 0000: Start MAP

This MAP describes initial fault isolation for the switch. Fault isolation begins at the HP StorageWorks High Availability Fabric Manager (HAFM) server, failed switch, or Internet-connected personal computer (PC) running the Embedded Web Server interface.

1

Prior to fault isolation, acquire the following information from the customer:

- A system configuration drawing or planning worksheet that includes the HAFM server, switches, other HP products, and device connections.
- The location of the HAFM server and all switches.
- The internet protocol (IP) address, gateway address, and subnet mask for the switch reporting the problem.
- If performing fault isolation using the HAFM server:
  - — The Windows 2000 user name and password. These are required when prompted during any MAP or repair procedure that directs the HAFM server to be rebooted.
  - — The user name, maintenance password, and HAFM server name. All are case sensitive and required when prompted at the **HAFM Login** dialog box.

- If performing fault isolation using the Embedded Web Server interface, the switch user name and password. Both are case sensitive and required when prompted at the **Username and Password Required** dialog box.

Continue.

2

Are you at the HAFM server?

YES **NO**

↓ **Go to** step 24**.**

3

Did the HAFM server lock up or crash and:

- Display an application warning or error message, or
- Not display an application warning or error message, or
- Display a **Dr. Watson for Windows 2000** dialog box?

NO **YES**

↓ An *HAFM server* application problem is indicated. Event codes are not recorded. Go to "MAP 0300: Console Application Problem Determination" on page 2-33.

4

Did the HAFM server crash and display a blue screen with the system dump file in hexadecimal format (blue screen of death)?

NO **YES**

↓ An *HAFM server* application problem is indicated. Event codes are not recorded. Go to "MAP 0300: Console Application Problem Determination" on page 2-33.

5

Is the *HAFM* application active?

NO **YES**

↓ **Go to** step 7**.**

6

Reboot the HAFM server PC.

a. Click the **Windows Start** button. The **Windows Workstation** menu displays.

b. At the **Windows Workstation** menu, select **Shut Down**. The **Shut Down Windows** dialog box displays.

c. At the **Shut Down Windows** dialog box, select **Shut down the Computer** and click **Yes** to power off the PC.

d. Wait approximately 30 seconds and power on the PC. After POSTs complete, the **Begin Logon** dialog box displays.

e. Simultaneously press **Ctrl**, **Alt**, and **Delete** to display the **Logon Information** dialog box. Type a user name and password (obtained in step 1) and click **OK**. The *HAFM Services* and *HAFM* applications start, and the **HAFM Login** dialog box displays.

f. At the **HAFM Login** dialog box, type a user name, password, and HAFM server name (obtained in step 1, and all are case sensitive), and click **Login**. The application opens and the **Product View** displays.

Did the **Product View** display and does the *HAFM* application appear operational?

YES **NO**

↓ An HAFM server hardware problem is indicated. Event codes are not recorded. Go to "MAP 0800: Console PC Problem Determination" on page 2-90.

7

Inspect the alert panel at the lower left corner of the **Product View**. The indicator shows the status of managed switches or the status of the link between the HAFM server and managed switches as follows:

- A green circle indicates all switches are operational.
- A yellow triangle indicates at least one switch is operating in degraded mode.
- A red diamond with yellow background indicates at least one switch is not operational.
- A grey square indicates the status of at least one switch is unknown

The grey square indicates the HAFM server cannot communicate with the switch because:

- The switch-to-HAFM server Ethernet link failed.
- Ac power distribution in the switch failed.
- The control processor (CTP) card failed. Because the CTP card is not a FRU, CTP failure requires replacing the switch.

Is a grey square displayed at the alert panel and as the background to the icon representing the switch reporting the problem?

YES **NO**

↓ **Go to** step 10**.**

8

At the switch reporting the problem, ensure the power switch is set to the Power On (1) position. Inspect the switch for indications of being powered on, such as:

- At the front panel, an illuminated PWR or ERR indicator.
- Green LEDs illuminated on the power supplies.
- Audio emanations and airflow from fans.

Does the switch appear powered on?

YES **NO**

↓ A power distribution problem is indicated. Go to step 23 to obtain event codes. If no event codes are found, go to "MAP 0100: Power Distribution Analysis" on page 2-26.

9

Either a switch-to-HAFM server Ethernet link failure or CTP failure is indicated. Go to step 23 to obtain event codes. If no event codes are found:

a. Fault isolate the least severe failure indicated (Ethernet link problem). Go to "MAP 0400: Loss of Console Communication" on page 2-39.

b. If MAP 400 does not isolate the problem, fault isolate the CTP problem. Go to "MAP 0200: POST, Reset, or IPL Failure Analysis" on page 2-32.

10

Is a red diamond with yellow background (failure indicator) displayed at the alert panel and as the background to the icon representing the switch reporting the problem?

YES **NO**

↓ **Go to** step 14.

11

Click the icon representing the switch reporting the problem. The **Hardware View** displays. At the **Hardware View**:

- Observe whether the Edge Switch 2/32 **Status** table is yellow and switch status is **NOT OPERATIONAL**.
- Inspect FRUs for a blinking red and yellow diamond (failed FRU indicator) that overlays a FRU graphic.

Does a blinking red and yellow diamond overlay a Fibre Channel port graphic?

NO **YES**

↓ A port SFP failure is indicated. **Go to** step 23 to obtain event codes. If no event codes are found, go to "MAP 0600: Port Failure and Link Incident Analysis" on page 2-63.

12

Does a blinking red and yellow diamond overlay a fan graphic?

NO **YES**

↓ A fan failure is indicated. **Go to** step 23 to obtain event codes. If no event codes are found, go to "MAP 0500: Fan and CTP Failure Analysis" on page 2-58.

13

A blinking red and yellow diamond overlays a power supply graphic.

A power supply failure is indicated. **Go to** step 23 to obtain event codes. If no event codes are found, go to "MAP 0100: Power Distribution Analysis" on page 2-26.

14

Is a yellow triangle (attention indicator) displayed at the alert panel and as the background to the icon representing the switch reporting the problem?

YES **NO**

↓ **Go to** step 18.

15

Click the icon representing the switch reporting the problem. The **Hardware View** displays. At the **Hardware View**:

- Observe whether the Edge Switch 2/32 **Status** table is yellow and switch status is **Minor Failure** or **Not Installed**.
- Inspect FRUs for a blinking red and yellow diamond (failed FRU indicator) that overlays the FRU graphic.

Does a blinking red and yellow diamond overlay a Fibre Channel port graphic?

NO **YES**

↓ A port SFP failure is indicated. **Go to** step 23 to obtain event codes. If no event codes are found, go to "MAP 0600: Port Failure and Link Incident Analysis" on page 2-63.

16

Does a blinking red and yellow diamond overlay a fan graphic?

NO **YES**

↓ A fan failure is indicated. **Go to** step 23 to obtain event codes. If no event codes are found, go to "MAP 0500: Fan and CTP Failure Analysis" on page 2-58.

17

A blinking red and yellow diamond overlays a power supply graphic.

A power supply failure is indicated. **Go to** step 23 to obtain event codes. If no event codes are found, go to "MAP 0100: Power Distribution Analysis" on page 2-26.

18

A green circle displays at the alert panel and as the background to the icon representing the switch reporting the problem. Although the switch is operational, a minor problem may exist.

Click the icon representing the switch reporting the problem. The **Hardware View** displays. At the **Hardware View**, inspect ports for a yellow triangle (attention indicator) that overlays a port graphic.

Does a yellow triangle overlay the port graphic?

YES **NO**

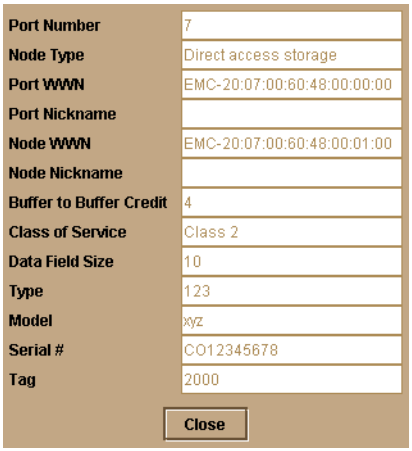
↓ **Go to** step 22.

19

Inspect the port state and LED status for all ports with an attention indicator.

a. At the **Hardware View**, click the port graphic with the attention indicator. The **Port Properties** dialog box displays.

b. Inspect the **Beaconing** and **Operational State** fields.



Does the **Operational State** field display a `Beaconing` message and the **Beaconing** field display an `On` message?

YES **NO**

↓ **Go to** step 21.

20

Port beaconing is enabled.

a. Consult with the customer and next level of support to determine the reason port beaconing is enabled.

b. Disable port beaconing:

   1. At the **Hardware View**, right-click the port graphic. A pop-up menu displays.
   2. Click **Enable Beaconing**. The check mark disappears from the box adjacent to the option, and port beaconing is disabled.

Was port beaconing enabled because port failure or degradation was suspected?

YES **NO**

↓ The switch appears operational.

Go to step 2.

21

At the **Port Properties** dialog box, does the **Operational State** field display a `Segmented E_Port` message?

NO **YES**

↓ E_Port segmentation is indicated. **Go to** step 23 to obtain event codes. If no event codes are found, go to "MAP 0700: Fabric, ISL, and Segmented Port Problem Determination" on page 2-79.

A message displays indicating a link incident or port problem. **Go to** step 23 to obtain event codes. If no event codes are found, go to "MAP 0600: Port Failure and Link Incident Analysis" on page 2-63.

22

A link incident may have occurred, but the LIN alerts option is not enabled for the port and the attention indicator does not display.

At the **Hardware View**, select **Link Incident Log** from the **Logs** menu on the navigation control panel. The **Link Incident Log** displays.

Date/Time	Port	Link Incident
3/31/02 12:21:56 PM	23	Loss-of-Signal or Loss-of-Synchronization.
3/22/02 4:09:11 PM	23	Not Operational primitive sequence (NOS) received.
3/22/02 4:09:11 PM	3	Not Operational primitive sequence (NOS) received.
3/22/02 4:07:38 PM	3	Not Operational primitive sequence (NOS) received.
3/22/02 4:07:10 PM	3	Loss-of-Signal or Loss-of-Synchronization.
3/22/02 3:06:09 PM	3	Not Operational primitive sequence (NOS) received.
3/22/02 3:06:09 PM	23	Not Operational primitive sequence (NOS) received.
3/21/02 4:34:52 PM	3	Loss-of-Signal or Loss-of-Synchronization.
3/21/02 4:30:11 PM	7	Not Operational primitive sequence (NOS) received.
3/21/02 4:29:13 PM	7	Loss-of-Signal or Loss-of-Synchronization.
3/21/02 4:19:41 PM	3	Not Operational primitive sequence (NOS) received.
3/21/02 3:47:51 PM	23	Not Operational primitive sequence (NOS) received.
3/21/02 10:28:38 AM	15	Not Operational primitive sequence (NOS) received.
3/21/02 10:28:28 AM	23	Loss-of-Signal or Loss-of-Synchronization.
3/21/02 10:27:03 AM	15	Loss-of-Signal or Loss-of-Synchronization.

Export... Clear Refresh Close

If a link incident occurred, the affected port number is listed with one of the following messages.

```
Link interface incident — implicit incident.

Link interface incident — bit-error threshold exceeded.

Link failure — loss of signal or loss of synchronization.

Link failure — not-operational primitive sequence (NOS)
received.
```

```
Link failure — primitive sequence timeout.

Link failure — invalid primitive sequence received for the
current link state.
```

Did one of the listed messages display in the Link Incident Log?

YES **NO**

↓ The switch appears operational.

A link incident problem is indicated. **Go to** step 23 to obtain event codes. If no event codes are found, go to "MAP 0600: Port Failure and Link Incident Analysis" on page 2-63.

23

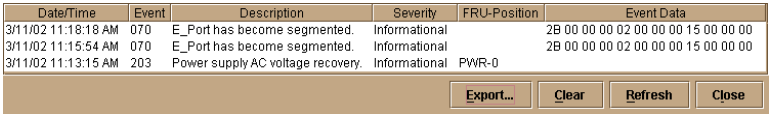
Obtain event codes from the switch Event Log.

NOTE: If multiple event codes are found, note all codes and associated severity levels. Record the date, time, and listed sequence, and determine if the codes are related to the reported problem. Begin fault isolation with the most recent event code with the highest severity level. Other codes may accompany this event code, or may indicate a normal indication after a problem is recovered.

a. At the **Hardware View**, select **Event Log** from the **Logs** menu on the navigation control panel. The **Event Log** displays.

b. Record the event code, date, time, and severity (**Informational**, **Minor**, **Major**, or **Severe**).

c. Record all event codes that may relate to the reported problem.



Date/Time	Event	Description	Severity	FRU-Position	Event Data
3/11/02 11:18:18 AM	070	E_Port has become segmented.	Informational		2B 00 00 00 02 00 00 00 15 00 00 00
3/11/02 11:15:54 AM	070	E_Port has become segmented.	Informational		2B 00 00 00 02 00 00 00 15 00 00 00
3/11/02 11:13:15 AM	203	Power supply AC voltage recovery.	Informational	PWR-0	

Export... Clear Refresh Close

Were one or more event codes found?

NO **YES**

↓ **Go to** Table 2–3 on page 2-2.

Return to the MAP step that sent you here.

24

Are you at the switch reporting the problem?

YES **NO**

↓ **Go to** step 36.

25

Is the PWR LED at the switch front panel illuminated?

NO **YES**

↓ **Go to** step 30.

26

Is the power switch set to the Power On (1) position?

NO **YES**

↓ **Go to** step 29.

27

Power on the switch. Inspect the switch for indications of being powered on, such as:

- At the front panel, an illuminated PWR or ERR indicator.
- Green LEDs illuminated on the power supplies.
- Audio emanations and airflow from fans.

Does the switch appear powered on?

YES **NO**

↓ A power distribution problem is indicated. **Go to** step 23 to obtain event codes. If no event codes are found, go to "MAP 0100: Power Distribution Analysis" on page 2-26.

28

Is the PWR LED at the switch front panel illuminated?

NO **YES**

↓ **Go to** step 30.

A faulty PWR LED is indicated, but Fibre Channel port operation is not disrupted.

a. If continued operation without benefit of the PWR LED is acceptable to the customer, do not perform any repair action.

b. If continued operation without benefit of the PWR LED is not acceptable to the customer, remove and replace the switch.

29

Inspect the switch for indications of being powered on, such as:

- At the front panel, an illuminated PWR or ERR indicator.
- Green LEDs illuminated on the power supplies.
- Audio emanations and airflow from fans.

Does the switch appear powered on?

YES **NO**

↓ A power distribution problem is indicated. **Go to** step 23 to obtain event codes. If no event codes are found, go to "MAP 0100: Power Distribution Analysis" on page 2-26.

A faulty PWR LED is indicated, but Fibre Channel port operation is not disrupted.

a. If continued operation without benefit of the PWR LED is acceptable to the customer, do not perform any repair action.

b. If continued operation without benefit of the PWR LED is not acceptable to the customer, remove and replace the switch.

Exit MAP.

30

Is the ERR LED blinking?

YES **NO**

↓ **Go to** step 32.

31

Unit beaconing is enabled for the switch.

a. Consult the customer and next level of support to determine the reason unit beaconing is enabled.

b. Disable unit beaconing.

1. At the **Hardware View**, right-click the front bezel graphic (away from a FRU). A pop-up menu displays.
2. Click **Enable Unit Beaconing**. The check mark disappears from the box adjacent to the option, and unit beaconing is disabled.

Was unit beaconing enabled because an switch failure or degradation was suspected?

YES **NO**

↓ The switch appears operational.

Go to step 25.

32

Is the **ERR** LED illuminated?

YES **NO**

↓ The switch appears operational. Verify operation at the HAFM server. **Go to** step 3.

33

Check FRUs (port SFPs, fans, power supplies) for failure symptoms.

Is the amber LED adjacent to a port SFP illuminated?

NO **YES**

↓ A port SFP failure is indicated. **Go to** step 23 to obtain event codes. If no event codes are found, go to "MAP 0600: Port Failure and Link Incident Analysis" on page 2-63.

34

Is the amber LED at the lower left corner of a fan illuminated?

NO **YES**

↓ A fan failure is indicated. **Go to** step 23 to obtain event codes. If no event codes are found, go to "MAP 0500: Fan and CTP Failure Analysis" on page 2-58.

35

Is the green LED on a power supply extinguished?

NO **YES**

↓ A power supply failure is indicated. **Go to** step 23 to obtain event codes. If no event codes are found, go to "MAP 0100: Power Distribution Analysis" on page 2-26.

The switch appears operational.

36

Are you at a PC with a web browser (such as Netscape Navigator or Microsoft Internet Explorer) and an Internet connection to the switch reporting the problem.

YES **NO**

↓ **Go to** step 52.

37

Is the web browser PC powered on and communicating with the switch through the Internet connection?

NO **YES**

↓ **Go to** step 39.

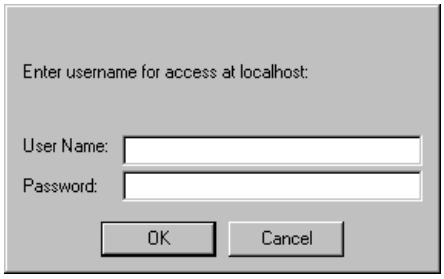
38

Boot the web browser PC.

a. Power on the PC in accordance with the instructions delivered with the PC. The Windows desktop displays.

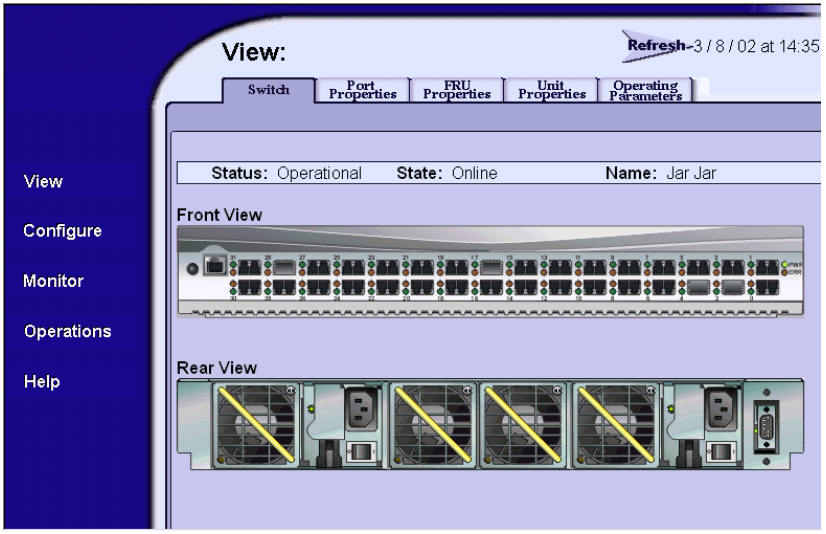
b. Launch the PC browser application by double-clicking the appropriate icon at the Windows desktop.

c. At the **Netsite** field (Netscape Navigator) or **Address** field (Internet Explorer), type `http://xxx.xxx.xxx.xxx`, where `xxx.xxx.xxx.xxx` is the IP address of the switch (obtained in step 1). The **Username and Password Required** dialog box displays.



d. Type the user name and password obtained in step 1, and click **OK**. The Embedded Web Server interface opens with the **View** panel (**Switch** tab) displayed.

Continue.



39

Does the Embedded Web Server interface appear operational with the **View** panel displayed?

NO **YES**

↓ **Go to** step 44**.**

40

A `Page cannot be found, Unable to locate the server, HTTP 404 — file not found`, or other similar message displays. The message indicates the web browser PC cannot communicate with the switch because:

- The switch-to-PC Internet link could not be established.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch's CTP failed. Because the CTP card is not a FRU, CTP failure requires replacing the switch.

Continue.

41

Inspect the switch for indications of being powered on, such as:

- At the front panel, an illuminated PWR or ERR indicator.

- Green LEDs illuminated on the power supplies.
- Audio emanations and airflow from fans.

Does the switch appear powered on?

YES **NO**

↓ A power distribution problem is indicated. Go to "MAP 0100: Power Distribution Analysis" on page 2-26.

42

Either a switch-to-PC Internet link problem (Internet too busy or IP address typed incorrectly) or a CTP failure is indicated.

a. Wait approximately five minutes, then attempt to login to the switch again.

b. At the **Netsite** field (Netscape Navigator) or **Address** field (Internet Explorer), type `http://xxx.xxx.xxx.xxx`, where `xxx.xxx.xxx.xxx` is the IP address of the switch (obtained in step 1). The **Username and Password Required** dialog box displays.

c. Type the user name and password obtained in step 1, and click **OK**. If the **View** panel does not display, wait another five minutes and perform this step again.

Does the Embedded Web Server interface appear operational with the **View** panel displayed?

YES **NO**

↓ A CTP failure is indicated. Go to "MAP 0200: POST, Reset, or IPL Failure Analysis" on page 2-32.

43

At the **View** panel, inspect the **Status** field.

Does the switch status indicate `Operational`?

NO **YES**

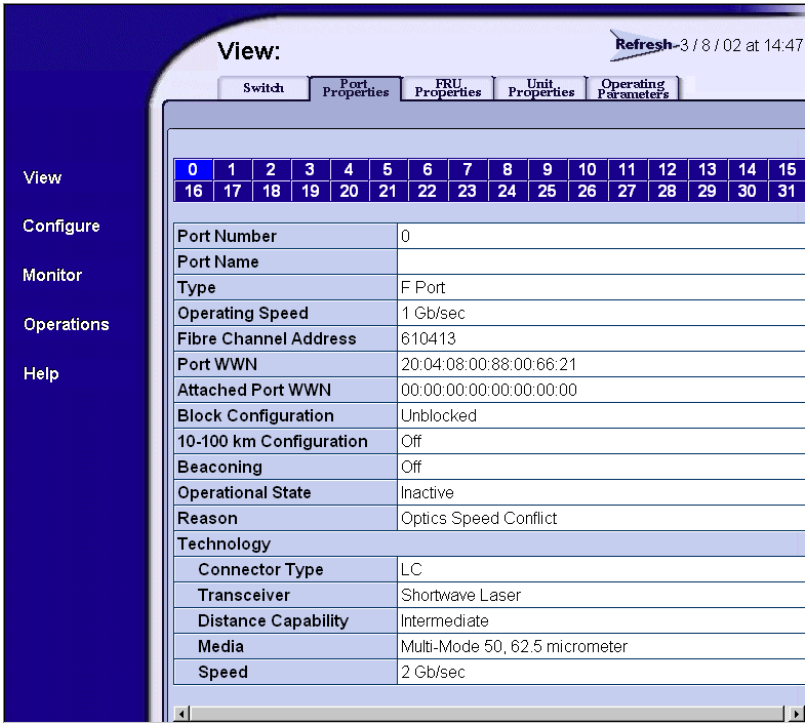
↓ The switch appears operational.

44

Inspect the port operational state.

a. At the **View** panel, click the **Port Properties** tab. The **View** panel (**Port Properties** tab) displays.

b. Inspect the **Beaconing** and **Operational State** fields.



Does the **Operational State** field display a `Beaconing` message and the **Beaconing** field display an `On` message?

YES **NO**

↓ **Go to** step 46.

45

Port beaconing is enabled.

a. Consult the customer and next level of support to determine the reason port beaconing is enabled.

b. Disable port beaconing:

1. At the **View** panel, select **Operations** at the left side of the panel. The **Operations** panel opens with the **Port Beaconing** page displayed.

2. Click the **Beaconing State** check box for the port. The check mark disappears from the box and port beaconing is disabled.
3. Return to the **View** panel (**Port Properties** tab).

Continue.

46

At the **View** panel, does the **Operational State** field display a `Segmented` message?

NO **YES**

↓ Port segmentation is indicated. **Go to** step 51 to obtain event codes. If no event codes are found, go to "MAP 0700: Fabric, ISL, and Segmented Port Problem Determination" on page 2-79.

47

At the **View** panel, does the **Operational State** field display a message indicating a link incident or port problem?

NO **YES**

↓ A port problem is indicated. **Go to** step 51 to obtain event codes. If no event codes are found, go to "MAP 0600: Port Failure and Link Incident Analysis" on page 2-63.

48

Repeat step 44 through step 47 for each remaining port.

Is a link incident or port problem indicated for any of the ports?

NO **YES**

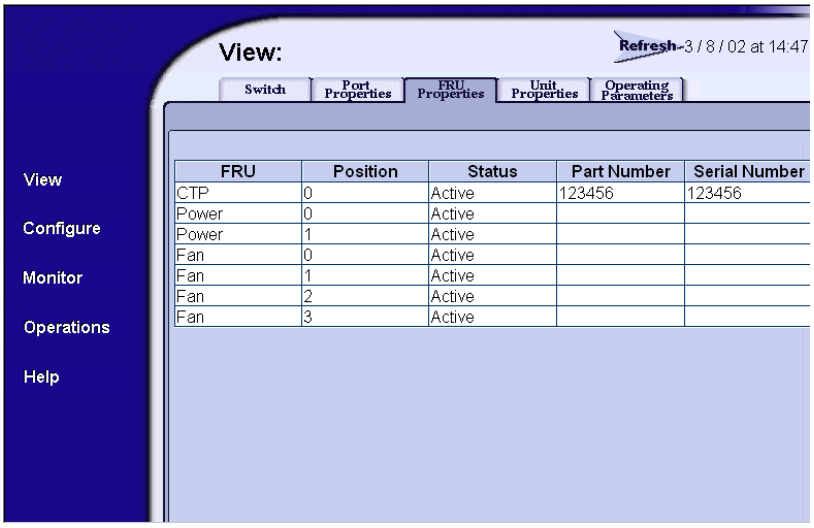
↓ A link incident problem or port SFP failure is indicated. **Go to** step 51 to obtain event codes. If no event codes are found, go to "MAP 0600: Port Failure and Link Incident Analysis" on page 2-63.

49

Inspect the power supply operational states.

a. At the **View** panel, click the **Component Properties** tab. The **View** panel (**Component Properties** tab) displays.

b. Inspect the **State** fields for both power supplies.



Does the **State** field display a `Failed` message for either power supply?

NO **YES**

↓ A power supply failure is indicated. **Go to** step 51 to obtain event codes. If no event codes are found, go to "MAP 0100: Power Distribution Analysis" on page 2-26.

50

Inspect the **State** fields for Fan 0, and Fan 1 through Fan 3 (fans).

Does the **State** field display a `Failed` or `Not Installed` message for any of the fans?

YES **NO**

↓ The switch appears operational.

A fan failure is indicated. Continue to the next step to obtain event codes. If no event codes are found, go to "MAP 0500: Fan and CTP Failure Analysis" on page 2-58.

51

Obtain event codes from the Embedded Web Server event log.

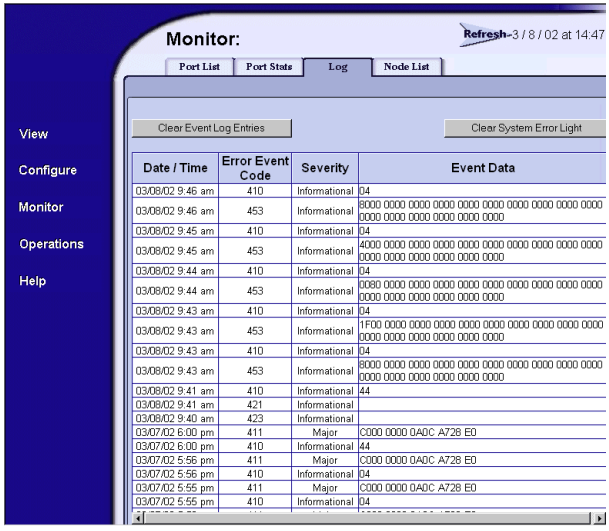
NOTE: If multiple event codes are found, note all codes and associated severity levels. Record the date, time, and listed sequence, and determine if the codes are related to the reported problem. Begin fault isolation with the most recent event code with the highest severity level. Other codes may accompany this event code, or may indicate a normal indication after a problem is recovered.

a. At the **View** panel, select **Monitor** at the left side of the panel. The **Monitor** panel opens with the **Status** page displayed.

b. At the **Monitor** panel, click the **Log** tab. The **Monitor** panel (**Log** tab) displays.

c. Record the event code, date, time, and severity (Informational, Minor, Major, or Severe).

d. Record all event codes that may relate to the reported problem.



Were one or more event codes found?

YES **NO**

↓ Return to the MAP step that sent you here.

Go to Table 2–3 on page 2-2.

52

The link incident record provides the attached switch port number(s) and one or more of the following event codes and messages. Record all event codes that may relate to the reported problem.

581 — Link interface incident **—** implicit incident.

582 — Link interface incident — bit-error threshold exceeded.

583 — Link failure — loss of signal or loss of synchronization.

584 — Link failure — not-operational primitive sequence (NOS) received.

585 — Link failure — primitive sequence timeout.

586 — Link failure — invalid primitive sequence received for the current link state.

Were one or more event codes found?

YES **NO**

↓ Perform switch fault isolation at the HAFM server.
Go to step 3.

Go to Table 2–3 on page 2-2.

MAP 0100: Power Distribution Analysis

This MAP describes fault isolation for the switch power distribution system, including defective AC power cords or power supplies.

1

Was an event code **200**, **201**, **202,** or **208** observed at the switch Event Log (HAFM server) or at the Embedded Web Server event log?

YES **NO**

↓ **Go to** step 3.

2

The following table lists event codes, brief explanations of the codes, and the associated steps that describe fault isolation procedures.

Event Code	Explanation	Action
200	Power supply AC voltage failure.	Go to step 6.
201	Power supply DC voltage failure.	Go to step 10.
202	Power supply thermal failure.	Go to step 10.
208	Power supply false shutdown.	Go to step 6.

3

Is remote fault isolation being performed at the HAFM server?

YES **NO**

↓ Remote fault isolation is being performed through the Embedded Web Server interface. **Go to** step 20.

4

Does inspection of a power supply indicate a failure (green LED extinguished)?

NO **YES**

↓ **Go to** step 6.

5

Does a blinking red and yellow diamond (failed FRU indicator) overlay a power supply graphic at the HAFM server **Hardware View**?

YES **NO**

↓ **Go to** step 11.

6

A redundant power supply is disconnected from facility AC power, not properly installed, or has failed.

Verify the indicated power supply is connected to facility power.

Ensure the AC power cord (PS0 or PS1) is connected to the rear of the switch and a facility power receptacle. If not, connect the cord as directed by the customer.

a. Ensure the associated facility circuit breaker is on. If not, ask the customer set the circuit breaker on.

b. Ensure the AC power cord is not damaged. If damaged, replace the cord.

Was a corrective action performed?

YES **NO**

↓ **Go to** step 8.

7

Verify power supply operation.

a. Inspect the power supply and ensure the green LED illuminates.

b. At the **Hardware View**, observe the graphic representing the power supply and ensure a failure symbol (blinking red and yellow diamond) does not display.

Is a failure indicated?

YES **NO**

↓ The switch appears operational.

8

Ensure the power supply is correctly installed and seated in the CTP card. If required, partially remove and reseat the power supply.

Was a corrective action performed?

YES **NO**

↓ **Go to** step 10.

9

Verify power supply operation.

a. Inspect the power supply and ensure the green LED illuminates.

b. At the **Hardware View**, observe the graphic representing the power supply and ensure a failure symbol (blinking red and yellow diamond) does not display.

Is a failure indicated?

YES **NO**

↓ The switch appears operational.

10

A redundant power supply failed and must be removed and replaced. (RRP: Power Supply on page 4-4).

- This procedure is concurrent and can be performed while the switch is powered on.
- Perform the data collection procedure after FRU removal and replacement.

Did power supply replacement solve the problem?

NO **YES**

↓ The switch appears operational.

Contact the next level of support.

11

At the **Product View**, is a grey square displayed at the alert panel and as the background to the icon representing the switch reporting the problem?

The grey square indicates the HAFM server cannot communicate with the switch because:

- The switch-to-HAFM server Ethernet link failed.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch's CTP failed. Because the CTP card is not a FRU, CTP failure requires replacing the switch.

YES **NO**

↓ The switch appears operational.

12

Ensure the power switch is set to the Power On (1) position. Inspect the switch for indications of being powered on, such as:

- At the front panel, an illuminated PWR or ERR indicator.
- Green LEDs illuminated on the power supplies.
- Audio emanations and airflow from fans.

Does the switch appear powered on?

NO **YES**

↓ Analysis for an Ethernet link or CTP failure is not described in this MAP. Go to "MAP 0000: Start MAP" on page 2-7. If this is the second time at this step, contact the next level of support.

13

Verify facility AC power connections.

a. Ensure both AC power cords (PS0 and PS1) are connected to the rear of the switch and to facility power receptacles. If not, connect the cords as directed by the customer.

b. Ensure associated facility circuit breakers are on. If not, ask the customer set the circuit breakers on.

c. Ensure the AC power cords are not damaged. If damaged, replace the cords.

Was a corrective action performed?

YES **NO**

↓ **Go to** step 15.

14

Verify operation of both power supplies.

a. Inspect the power supplies and ensure the green LEDs illuminate.

b. At the **Hardware View**, observe the graphics representing the power supplies and ensure a failure symbol (blinking red and yellow diamond) does not display.

Is a failure indicated?

YES **NO**

↓ The switch appears operational.

15

Ensure both power supplies are correctly installed and seated in the CTP card. If required, partially remove and reseat the power supplies.

Was a corrective action performed?

YES **NO**

↓ **Go to** step 17.

16

Verify operation of both power supplies.

a. Inspect the power supplies and ensure the green LEDs illuminate.

b. At the **Hardware View**, observe the graphics representing the power supplies and ensure a failure symbol (blinking red and yellow diamond) does not display.

Is a failure indicated?

YES **NO**

↓ The switch appears operational.

17

Inspect the switch for indications the power supplies are operational, but the switch is not receiving DC power. Indications include:

- Green LEDs illuminated on one or both power supplies.
- PWR and ERR LEDS extinguished at the switch front panel.

- All green and amber port LEDs extinguished.

Does the switch appear powered off while the power supplies appear operational (one or both power supply LEDs illuminated)?

NO **YES**

↓ **Go to** step 19.

18

Both power supplies failed and must be removed and replaced (RRP: Power Supply on page 4-4). Perform the data collection procedure after FRU removal and replacement.

Did replacement of both power supplies solve the problem?

NO **YES**

↓ The switch appears operational.

Contact the next level of support.

19

One or both power supplies appear operational, but the CTP is not receiving DC power. An in-card circuit breaker may have tripped due to a power surge or the CTP failed.

Reset the switch ("Reset the Switch" on page 3-36).

Did a switch reset solve the problem?

NO **YES**

↓ The switch appears operational.

A CTP failure is indicated. Because the CTP card is not a FRU, CTP failure requires replacing the switch.

20

Does the Embedded Web Server interface appear operational?

NO **YES**

↓ **Go to** step 22.

21

A `Page cannot be found, Unable to locate the server, HTTP 404 — file not found`, or other similar message displays. The message indicates the web browser PC cannot communicate with the switch because:

- The switch-to-PC Internet (Ethernet) link could not be established.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP failed.

Go to step 12.

22

Inspect the power supply operational states at the Embedded Web Server interface.

a. At the **View** panel, click the **Component Properties** tab. The **View** panel (**Component Properties** tab) displays.

b. Inspect the **State** fields for Power Supply 0 and Power Supply 1.

Does the **State** field display a `Failed` or `Not Installed` message for either power supply?

NO **YES**

↓ A redundant power supply failure is indicated. **Go to** step 6.

The switch appears operational.

MAP 0200: POST, Reset, or IPL Failure Analysis

When the switch is powered on, it performs a series of power-on self-tests (POSTs). When POSTs complete, the switch performs an initial program load (IPL) that loads firmware and brings the unit online. This MAP describes fault isolation for problems that may occur during the POST/IPL process.

If an error is detected, the POST/IPL process continues in an attempt to initialize the switch and bring it online. But an event code **400** displays when the switch completes the POST/IPL process.

1

Was an event code **400** or **411** observed at the switch Event Log (HAFM server) or at the Embedded Web Server event log?

YES **NO**

↓ Analysis for the failure is not described in this MAP. Go to "MAP 0000: Start MAP" on page 2-7.

2

The following table lists event codes, brief explanations of the codes, and the associated steps that describe fault isolation procedures.

Event Code	Explanation	Action
400	Power-up diagnostic failure.	Go to step 3.
411	Firmware fault occurred.	Go to step 4.

3

POST/IPL diagnostics detected a CTP failure as indicated by an event code **400** with supplementary bytes of event data.

- Byte 0 is a FRU code (02) that indicates a failed CTP.
- Byte 1 is the slot number (00) for the CTP.

Because the CTP card is not a FRU, CTP failure requires replacing the switch.

4

POST/IPL diagnostics detected a firmware failure (as indicated by event code **411**) and performed an online dump. All Fibre Channel ports reset after the failure and attached devices momentarily logout, login, and resume operation.

Perform the data collection procedure and return the Zip disk to HP support personnel.

MAP 0300: Console Application Problem Determination

This map describes isolation of *HAFM server* application problems, including problems associated with the Windows operating system and HAFM and switch Product Manager.

1

Did the HAFM server lock up or crash without displaying a warning or error message?

YES **NO**

↓ **Go to** step 4.

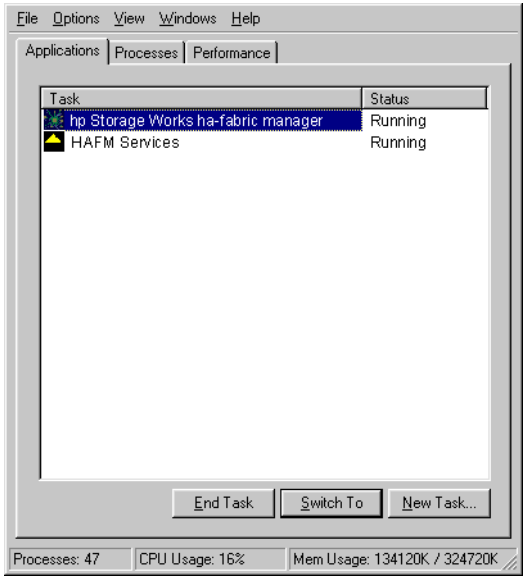
2

An application or operating system problem is indicated. Close the *HAFM* application.

a. Simultaneously press **Ctrl**, **Alt**, and **Delete**. The **Windows Security** dialog box displays.

b. At the **Windows Security** dialog box, click **Task Manager**. The **Windows Task Manager** dialog box displays with the **Applications** page open.

c. Select (highlight) **HP StorageWorks High Availability Fabric Manager** and click **End Task**. The *HAFM* application closes.



Continue.

3

Attempt to clear the problem by rebooting the HAFM server PC.

a. Click the **Windows Start** button. The **Windows Workstation** menu displays.

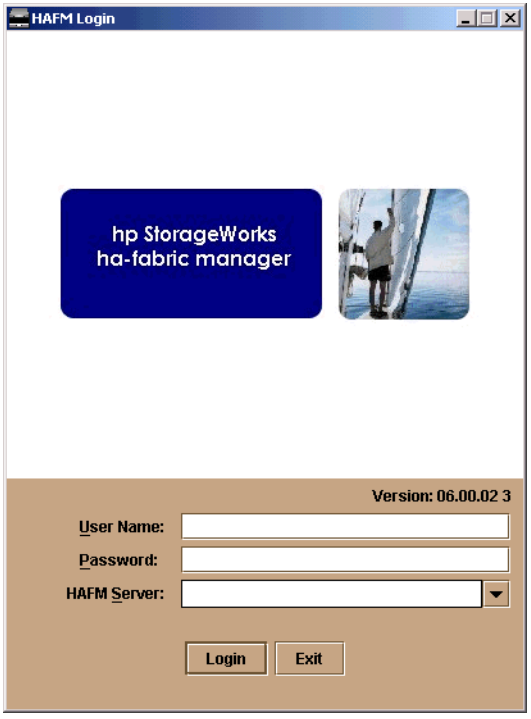
b. At the **Windows Workstation** menu, select **Shut Down**. The **Shut Down Windows** dialog box displays.

c. At the **Shut Down Windows** dialog box, select **Shut down the Computer** and click **Yes** to power off the PC.

d. Wait approximately 30 seconds and power on the PC. After POSTs complete, the **Begin Logon** dialog box displays.

e. Simultaneously press **Ctrl**, **Alt**, and **Delete** to display the **Logon Information** dialog box. Type a user name and password (obtained in "MAP 0000: Start MAP" on page 2-7) and click **OK**. The *HAFM* application starts and the **HAFM Login** dialog box displays.

f. At the **HAFM Login** dialog box, type a user name, password, and HAFM server name (obtained in "MAP 0000: Start MAP" on page 2-7) and click **Login**. The application opens and the **Product View** displays.



Did the **Product View** display and does the *HAFM* application appear operational?

NO **YES**

↓ The problem is transient and the HAFM server appears operational.

Contact the next level of support.

4

Did the *HAFM* application display a dialog box with the message `Connection to HAFM server lost — click OK to exit application or HAFM error n` (where `n` is an error message number 1 through 8 inclusive)?

NO **YES**

↓ An *HAFM* application error occurred. Click **OK** to close the dialog box and close the *HAFM* application. **Go to** step 3.

5

Did the *HAFM* application display a dialog box with the message `The software version on this HAFM server is not compatible with the version on the remote HAFM server`?

YES **NO**

↓ **Go to** step 8.

6

The *HAFM* applications running on the HAFM server and client workstation are not at compatible release levels. Recommend to the customer that the downlevel version be upgraded.

Does the customer want the *HAFM* application upgraded?

YES **NO**

↓ Power off the client workstation.

7

Upgrade the downlevel *HAFM* application ("Install or Upgrade Software" on page 3-51).

Did the software upgrade solve the problem?

NO **YES**

↓ The HAFM server appears operational

Contact the next level of support.

8

Did the *Product Manager* application display a dialog box with the message `Product Manager error 5001 or Product Manager error 5002`?

NO **YES**

↓ A *Product Manager* application error occurred. Click **OK** to close the dialog box and close the *HAFM* and *Product Manager* applications. **Go to** step 3.

9

Did the *Product Manager* application display a dialog box with the message `Send firmware failed`?

YES **NO**

↓ **Go to** step 11.

10

An attempt to download a firmware version from the HAFM server hard drive to the switch failed. Retry the operation ("Manage Firmware Versions" on page 3-40).

Did the firmware version download to the switch?

NO **YES**

↓ The HAFM server appears operational.

A CTP failure is suspected. Go to "MAP 0000: Start MAP" on page 2-7 to isolate the problem.

11

Did the *Product Manager* application display a dialog box with the message `The data collection process failed`?

YES **NO**

↓ **Go to** step 13.

12

The data collection process failed. Retry the process using a new Zip disk("Collecting Maintenance Data" on page 3-32).

Did the data collection process complete?

NO **YES**

↓ **Exit MAP.**

Contact the next level of support.

13

Did the HAFM server lock up or crash and display a **Dr. Watson for Windows** dialog box?

NO **YES**

↓ A Windows operating system or *HAFM* application error occurred. Click **Cancel** to close the dialog box and *HAFM* application. **Go to** step 3.

14

Did the HAFM server crash and display a blue screen with the system dump file in hexadecimal format (blue screen of death)?

YES **NO**

↓ The HAFM server appears operational.

15

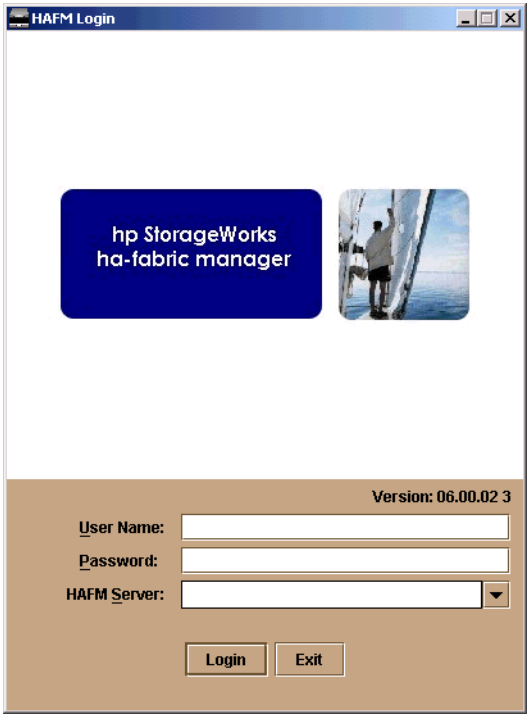
Attempt to clear the problem by power cycling the HAFM server PC.

a. Power off the PC.

b. Wait approximately 30 seconds and power on the PC. After POSTs complete, the **Begin Logon** dialog box displays.

c. Simultaneously press **Ctrl**, **Alt**, and **Delete** to display the **Logon Information** dialog box. Type a user name and password (obtained in "MAP 0000: Start MAP" on page 2-7) and click **OK**. The *HAFM* application starts and the **HAFM Login** dialog box displays.

d. At the **HAFM Login** dialog box, type a user name, password, and HAFM server name (obtained in "MAP 0000: Start MAP" on page 2-7), and click **Login**. The application opens and the **Product View** displays.



Did the **Product View** display and does the *HAFM* application appear operational?

NO **YES**

↓ The problem is transient and the HAFM server appears operational**.**

Contact the next level of support.

MAP 0400: Loss of Console Communication

This MAP describes fault isolation of the Ethernet communication link between a switch and the HAFM server, or between a switch and a web browser PC running the Embedded Web Server interface. Failure indicators include:

- At the **Product View**, a grey square at the alert panel and as the background to the icon representing the switch reporting the problem.
- At the **Hardware View**, a grey square at the alert panel, a **No Link** status and reason at the switch **Status** table, and no FRUs visible for the switch.
- At the web browser PC, A `Page cannot be found, Unable to locate the server, HTTP 404 — file not found`, or other similar message.
- An event code **433** recorded *only* in nonvolatile random-access memory (NV-RAM) on the switch's CTP card.
- An event code **430, 431, 432, 440** recorded at the switch *Event Log* or Embedded Web Server event log.

When the logical connection between the switch and HAFM server is initiated, it may take up to five minutes for the link to activate at the **Product View**, and a green circle to display at the alert panel and the background to the icon representing the switch. This delay is normal.

CAUTION: Prior to servicing a switch or HAFM server, determine the Ethernet LAN configuration. Installation of switches and the HAFM server on a public customer intranet can complicate problem determination and fault isolation.

1

Was an event code **430**, **431**, **432**, or **440** observed at the switch Event Log (HAFM server) or at the Embedded Web Server event log?

YES **NO**

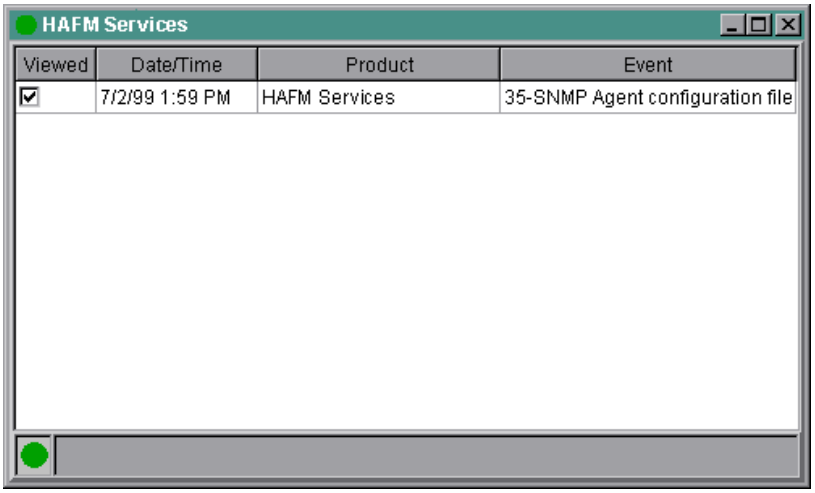
↓ **Go to** step 5.

2

A transmission control protocol (TCP) reset command from the HAFM server caused the Ethernet connection to terminate. The connection recovers if the HAFM server is powered on and the *HAFM Services* application is running.

Verify the HAFM server is powered on and the *HAFM* application is running. The application runs in the background as a Windows service and starts automatically when the HAFM server is powered on.

Click **HAFM Services** at the Windows task bar. The **HAFM Services** window displays.



Is the HAFM server powered on and the *HAFM* application running?

YES **NO**

↓ **Go to** step 4.

3

Did the switch-to-HAFM server Ethernet connection recover?

NO **YES**

↓ The switch-to-HAFM server connection is restored and appears operational.

Contact the next level of support.

4

Reboot the HAFM server PC.

a. Click the **Windows Start** button. The **Windows Workstation** menu displays.

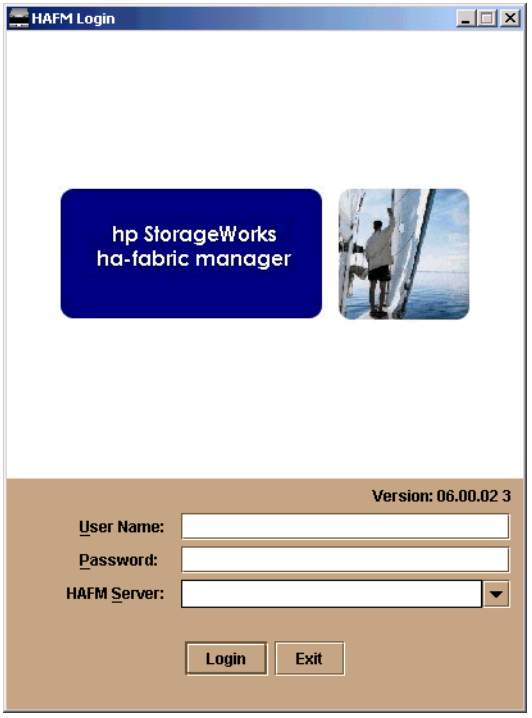
b. At the **Windows Workstation** menu, select **Shut Down**. The **Shut Down Windows** dialog box displays.

c. At the **Shut Down Windows** dialog box, select **Shut down the Computer** and click **Yes** to power off the PC.

d. Wait approximately 30 seconds and power on the PC. After POSTs complete, the **Begin Logon** dialog box displays.

e. Simultaneously press **Ctrl**, **Alt**, and **Delete** to display the **Logon Information** dialog box. Type a user name and password (obtained in "MAP 0000: Start MAP" on page 2-7) and click **OK**. The *HAFM* application starts and the **HAFM Login** dialog box displays.

f. At the **HAFM Login** dialog box, type a user name, password, and HAFM server name (obtained in "MAP 0000: Start MAP" on page 2-7), and click **Login**. The application opens and the **Product View** displays.



Did the switch-to-HAFM server Ethernet connection recover?

NO **YES**

↓ The switch-to-HAFM server connection is restored and appears operational.

Contact the next level of support.

5

Is fault isolation being performed at the switch or HAFM server?

YES **NO**

↓ Remote fault isolation is being performed through the Embedded Web Server interface. **Go to** step 25.

6

At the **Product View**, is a grey square displayed at the alert panel and as the background to the icon representing the switch reporting the problem?

YES **NO**

↓ The switch-to-HAFM server connection is restored and appears operational.

The grey square indicates the HAFM server cannot communicate with the switch because:

- The switch-to-HAFM server Ethernet link failed.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP card failed. Because the CTP card is not a FRU, replace the switch.

Continue.

7

Inspect the switch reporting the problem for indications of being powered on, such as:

- At the front panel, an illuminated PWR or ERR indicator.
- Green LEDs illuminated on the power supplies.
- Audio emanations and airflow from fans.

Does the switch appear powered on?

YES **NO**

↓ Analysis for an ac power distribution or CTP failure is not described in this MAP. Go to "MAP 0000: Start MAP" on page 2-7. If this is the second time at this step, contact the next level of support.

8

The switch-to-HAFM server Ethernet link failed. Click the icon with the grey square representing the switch reporting the problem. The **Hardware View** displays. At the **Hardware View**:

- A grey square displays at the alert panel.
- No FRUs are visible for the switch.
- The switch **Status** table is yellow, the **Status** field displays No Link, and the **Reason** field displays an error message.

The following table lists the error messages and associated steps that describe fault isolation procedures.

Error Message	Action
`Never connected.`	Go to step 9.
`Link timeout.`	Go to step 9.
`Protocol mismatch.`	Go to step 15.
`Duplicate session.`	Go to step 18.
`Unknown network address.`	Go to step 21.
`Incorrect product type.`	Go to step 23.

9

Errors for the switch Ethernet adapter exceeded a threshold, the switch-to-HAFM server link was not connected, or the switch-to-HAFM server link timed out. A problem with the Ethernet cable, hub or hubs, or other LAN-attached device is indicated.

Verify the switch is connected to the HAFM server through one or more Ethernet hubs.

a. Ensure an RJ-45 Ethernet cable connects the switch front panel to an Ethernet hub. If not, connect the cable as directed by the customer.

b. Ensure an RJ-45 Ethernet cable connects the HAFM server adapter card to an Ethernet hub. If not, connect the cable as directed by the customer.

c. Ensure both Ethernet cables are not damaged. If damaged, replace the cables.

Was a corrective action performed?

NO **YES**

↓ **Go to** step 1.

10

Does the LAN configuration use multiple Ethernet hubs that are daisy-chained?

YES **NO**

↓ **Go to** step 12.

11

Verify the hubs are correctly interconnected.

Was a corrective action performed?

NO **YES**

↓ **Go to** step 1.

12

Verify operation of the Ethernet hub or hubs. Inspect each hub for indications of being powered on, such as:

- Green Power LED illuminated.
- Green Status LEDs illuminated.

Is a hub failure indicated?

YES **NO**

↓ **Go to** step 14.

13

Replace the Ethernet hub. Refer to the supporting documentation shipped with the hub for instructions.

Did hub replacement solve the problem?

NO **YES**

↓ The switch-to-HAFM server connection is restored and appears operational.

A switch Ethernet port failure is indicated. **Go to** step 29.

14

A problem with another LAN-attached device is indicated.

- If the problem is associated with another switch or HAFM server, go to "MAP 0000: Start MAP" on page 2-7 to isolate the problem for that device.

- If the problem is associated with an unrelated device, notify the customer and have the system administrator correct the problem.

Did repair of an unrelated LAN-attached device solve the problem?

NO **YES**

↓ The switch-to-HAFM server connection is restored and appears operational.

A switch Ethernet port failure is indicated. **Go to** step 29.

15

The *HAFM* application (running on the HAFM server) and the firmware running on the switch are not at compatible release levels. Recommend to the customer that the downlevel version (software or firmware) be upgraded.

Does the *HAFM* application require upgrade?

YES **NO**

↓ **Go to** step 17.

16

At the HAFM server, upgrade the *HAFM* application ("Install or Upgrade Software" on page 3-51).

Did the switch-to-HAFM server Ethernet connection recover?

NO **YES**

↓ The switch-to-HAFM server connection is restored and appears operational.

Contact the next level of support.

17

A switch firmware upgrade is required.

Download the firmware ("Download a Firmware Version to a Switch" on page 3-46). After the download, perform the data collection procedure and return the Zip disk to HP for analysis.

Did the switch-to-HAFM server Ethernet connection recover?

NO **YES**

↓ The switch-to-HAFM server connection is restored and appears operational.

Contact the next level of support.

18

An instance of the *HAFM* application is open at another HAFM server and communicating with the switch. Notify the customer and either:

- Power off the HAFM server running the second instance of the application, or
- Configure the HAFM server running the second instance of the application as a client workstation.

Does the customer want the second HAFM server configured as a client?

YES **NO**

↓ Power off the HAFM server reporting the Duplicate Session communication problem.

19

Determine the internet protocol (IP) address of the HAFM server running the first instance of the *HAFM* application.

a. Click the **Windows Start** button. The **Windows Workstation** menu displays.

b. At the **Windows Workstation** menu, select **Settings**. From the menu that displays, select **Control Panel**. The **Control Panel** window displays.

c. At the **Control Panel** window, double-click the **Network** icon. The **Network** dialog box displays with the **Identification** page open.

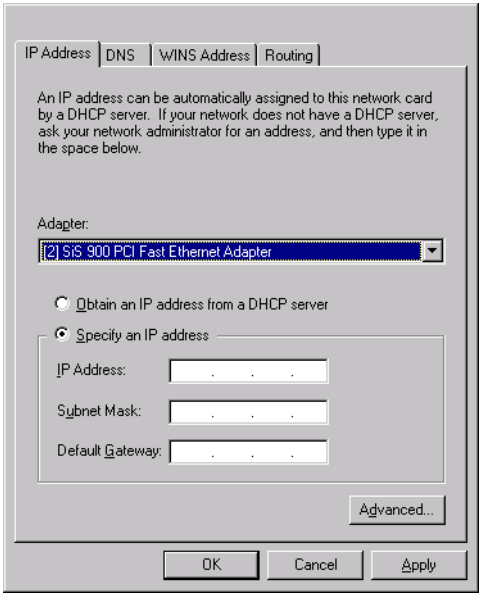
d. Click the **Protocols** tab. The **Protocols** page opens.

e. Select (highlight) **TCP/IP Protocol** from the list box and click **Properties**. The **Microsoft TCP/IP Properties** dialog box displays with the **IP Address** page open (as shown in the following figure).

f. Record the IP address, then click **OK** to close the dialog box.

g. At the **Network** dialog box, click **OK** to close the dialog box.

h. Close the **Control Panel** window.


IP Address
DNS
WINS Address
Routing
An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.
Adapter:
[2] SiS 900 PCI Fast Ethernet Adapter
Obtain an IP address from a DHCP server
Specify an IP address
IP Address:
Subnet Mask:
Default Gateway:
Advanced...
OK
Cancel
Apply

Continue.

20

Configure the HAFM server reporting the Duplicate Session communication problem as a client.

a. At the **Product View**, select **Logout** from the **Logout/Exit** menu on the navigation control panel. The **HAFM Login** dialog box displays.

b. At the **HAFM Login** dialog box, type a user name and password (obtained in "MAP 0000: Start MAP" on page 3-7).

c. Type the IP address of the HAFM server running the first instance of the *HAFM* application in the **HAFM server** field.

d. Click **Login**. The *HAFM* application opens as a client and the **Product View** displays.

Did the HAFM server reconfigure as a client and did the Ethernet connection recover?

NO **YES**

↓ The switch-to-HAFM server connection is restored and the second HAFM server appears operational as a client.

Contact the next level of support.

21

The IP address defining the switch to the *HAFM* application is incorrect or unknown and must be verified. A maintenance terminal (desktop or notebook PC) and asynchronous RS-232 modem cable are required to verify the switch IP address. Both tools are provided by installation or service personnel. To verify the switch IP address:

a. Remove the protective cap from the 9-pin maintenance port at the rear of the switch (a flat-tip screwdriver may be required). Connect one end of the RS-232 modem cable to the port.

b. Connect the other cable end to a 9-pin communication port (COM1 or COM2) at the rear of the maintenance terminal PC.

c. Power on the maintenance terminal. After the PC powers on, the Windows desktop displays.

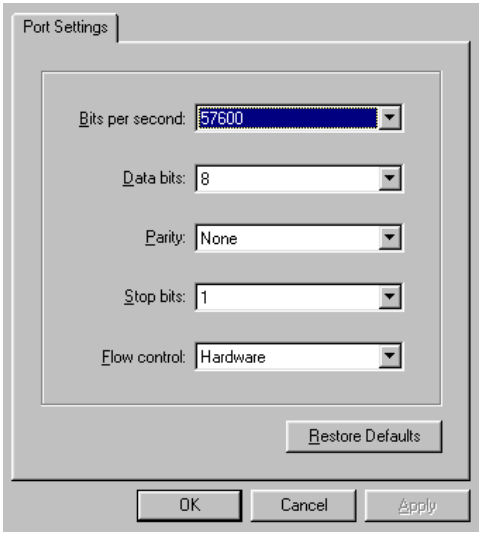
d. At the Windows desktop, click the **Windows Start** button. The **Windows Workstation** menu displays.

NOTE: The following steps describe inspecting the IP address using HyperTerminal serial communication software.

e. At the **Windows Workstation** menu, sequentially select **Programs**, **Accessories**, and **HyperTerminal**. The **Connection Description** dialog box displays.

f. Type `Edge-32` in the **Name** field and click **OK**. The **Connect To** dialog box displays.

g. Ensure the **Connect using** field displays `COM1` or `COM2` (depending on the serial communication port connection to the switch) and click **OK**. The **COMn** dialog box displays (where *n* is 1 or 2).



h. Configure the Port Settings parameters as follows:

— Bits per second — 57600.

— Data bits — 8.

— Parity — None.

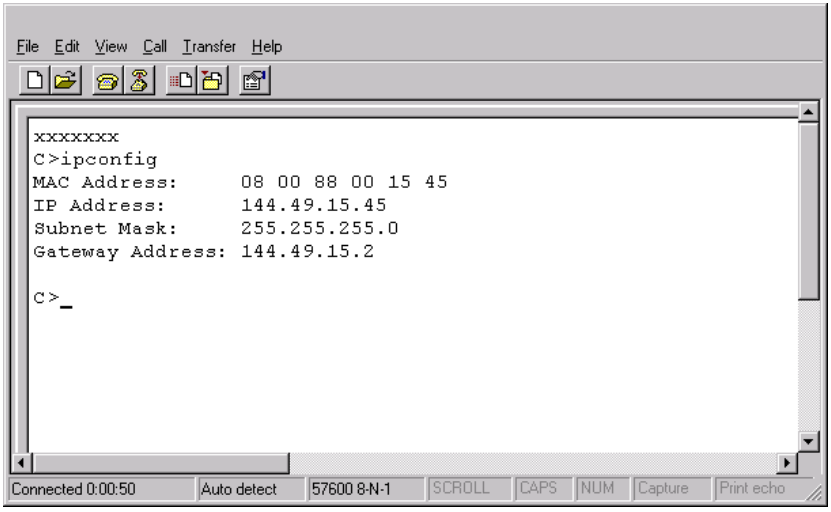
— Stop bits — 1.

— Flow control — Hardware.

When the parameters are set, click **OK**. The **HyperTerminal** window displays.

i. At the > prompt, type the user-level password (the default is password) and press **Enter**. The password is case sensitive. The HyperTerminal window displays with software and hardware version information for the switch, and an C> prompt at the bottom of the window.

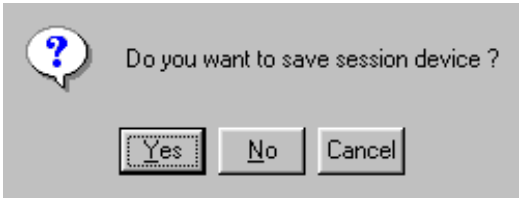
j. At the C> prompt, type the ipconfig command and press **Enter**. The HyperTerminal window displays with configuration information listed (including the IP address).



k. Record the switch IP address.

l. Select **Exit** from the **File** pull-down menu to close the *HyperTerminal* application. The following message box displays:

m. Click **Yes**. The following message box displays:



n. Click **No** to exit and close the *HyperTerminal* application.

o. Power off the maintenance terminal.

p. Disconnect the RS-232 modem cable from the switch and the maintenance terminal. Replace the protective cap over the maintenance port.

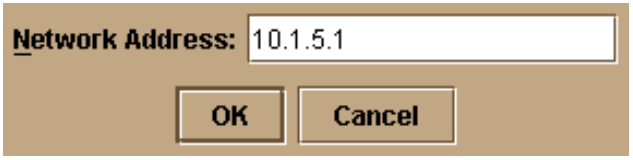
Continue.

22

Define the switch's correct IP address to the HAFM server.

a. At the **Product View**, right-click the icon with the grey square representing the switch reporting the problem. A pop-up menu displays.

b. Select **Modify**. The **Modify Network Address** dialog box displays.



c. Type the correct IP address and click **OK**.

Did the IP address below the switch icon change to the new entry and did the Ethernet connection recover?

NO **YES**

↓ The switch-to-HAFM server connection is restored and appears operational.

Contact the next level of support.

23

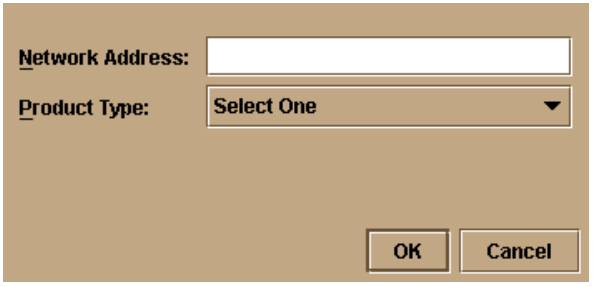
An incorrect product type is defined to the HAFM server

a. At the **Product View**, right-click the icon with the grey square representing the product reporting the problem. A pop-up menu displays.

b. Select **Delete**. A warning dialog box displays asking if the product is to be deleted.

c. Click **Yes** to delete the product.

d. At the **Product View**, select **New Product** from the **Configure** menu on the navigation control panel. The **New Product** dialog box displays.



e. Type the configured IP address in the **Network Address** field.

f. Select **Edge-32** from the **Product Type** list box and click **OK**.

Did the IP address below the switch icon change to the new entry and did the Ethernet connection recover?

NO **YES**

↓ The switch-to-HAFM server connection is restored and appears operational.

24

The product at the configured IP address is not an HP managed product. Notify the customer of the problem.

a. At the **Product View**, right-click the icon with the grey square representing the product reporting the problem. A pop-up menu displays.

b. Select **Delete**. A warning dialog box displays asking if the product is to be deleted.

c. Click **Yes** to delete the product.

Exit MAP.

25

Does the *Embedded Web Server* application appear operational?

NO **YES**

↓ The switch-to-web server PC connection is restored and appears operational.

26

A `Page cannot be found, Unable to locate the server, HTTP 404 — file not found`, or other similar message displays. The message indicates the web browser PC cannot communicate with the switch because:

- The switch-to-PC Internet (Ethernet) link could not be established.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP failed.

Continue.

27

Inspect the switch reporting the problem for indications of being powered on, such as:

- At the front panel, an illuminated PWR or ERR indicator.
- Green LEDs illuminated on the power supplies.
- Audio emanations and airflow from fans.

Does the switch appear powered on?

YES **NO**

↓ Analysis for an AC power distribution or CTP failure is not described in this MAP. Go to "MAP 0000: Start MAP" on page 2-7. If this is the second time at this step, contact the next level of support.

28

Either a switch-to-PC Internet link problem (Internet too busy or IP address typed incorrectly) or a switch Ethernet port failure is indicated.

a. Wait approximately five minutes, then attempt to login to the switch again.

b. At the **Netsite** field (Netscape Navigator) or **Address** field (Internet Explorer), type `http://xxx.xxx.xxx.xxx`, where `xxx.xxx.xxx.xxx` is the IP address of the switch (obtained in "MAP 0000: Start MAP" on page 2-7). The **Username and Password Required** dialog box displays.

c. Type the user name and password (obtained in "MAP 0000: Start MAP" on page 2-7) and click **OK**. If the **View** panel does not display, wait another five minutes and perform this step again.

Does the Embedded Web Server interface appear operational with the **View** panel displayed?

NO **YES**

↓ The switch-to-web server PC connection is restored and appears operational.

29

An unrecoverable Ethernet fault (reported as event code **433**) is indicated. The event code is not reported to the switch Event Log or the Embedded Web Server event log, and must be verified through the switch maintenance port. A maintenance terminal (desktop or notebook PC) and asynchronous RS-232 modem cable are required to verify the reporting of event code **433**. Both tools are provided by installation or service personnel. To verify the event code:

a. Remove the protective cap from the 9-pin maintenance port at the rear of the switch (a flat-tip screwdriver may be required). Connect one end of the RS-232 modem cable to the port.

b. Connect the other cable end to a 9-pin communication port (COM1 or COM2) at the rear of the maintenance terminal PC.

c. Power on the maintenance terminal. After the PC powers on, the Windows desktop displays.

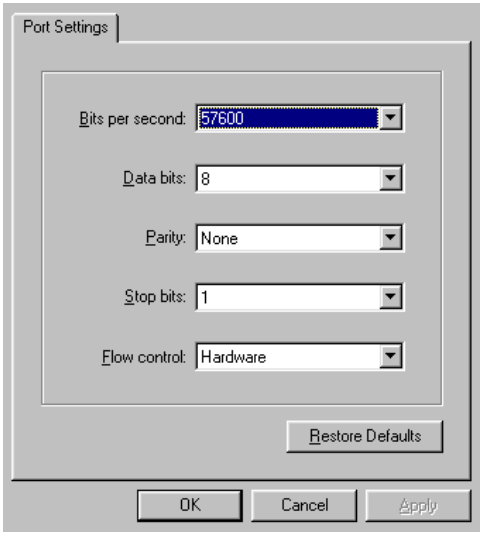
d. At the Windows desktop, click the **Windows Start** button. The **Windows Workstation** menu displays.

NOTE: The following steps describe inspecting event code **433** using HyperTerminal serial communication software.

e. At the **Windows Workstation** menu, sequentially select **Programs**, **Accessories**, and **HyperTerminal**. The **Connection Description** dialog box displays.

f. Type `Edge-32` in the **Name** field and click **OK**. The **Connect To** dialog box displays.

g. Ensure the **Connect using** field displays `COM1` or `COM2` (depending on the serial communication port connection to the switch), and click **OK**. The **COMn** dialog box displays (where *n* is 1 or 2).



h. Configure the Port Settings parameters as follows:

— Bits per second — 57600.

— Data bits — 8.

— Parity — None.

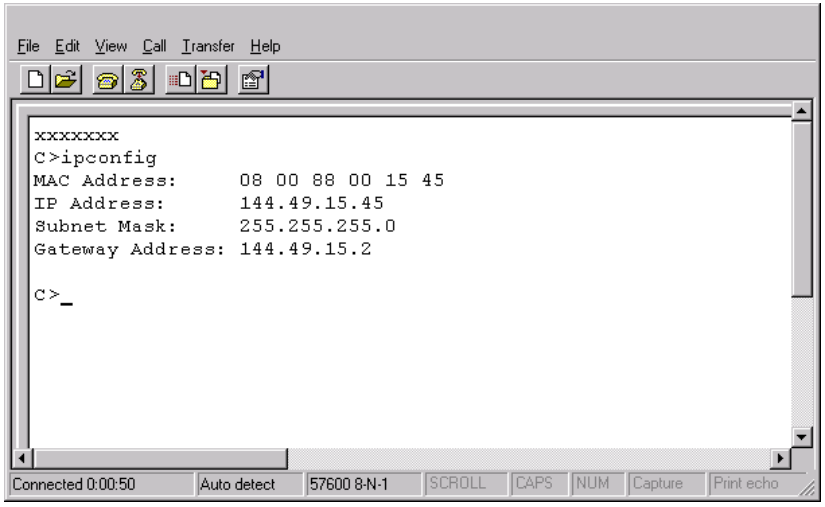
— Stop bits — 1.

— Flow control — Hardware.

When the parameters are set, click **OK**. The **HyperTerminal** window displays.

i. At the C> prompt, type the user-level password (the default is password) and press **Enter**. The password is case sensitive. The HyperTerminal window displays with software and hardware version information for the switch, and a C> prompt at the bottom of the window.

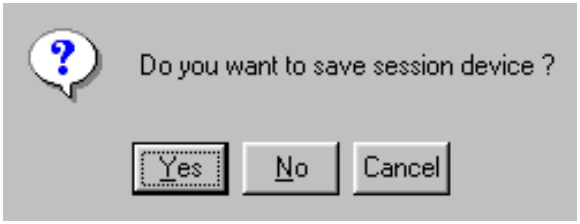
j. At the C> prompt, type the displaylog command and press **Enter**. The HyperTerminal window displays with the event log (from switch NV-RAM) listed.



k. If listed in the **REAS** column, record the event code **433**.

l. Select **Exit** from the **File** pull-down menu to close the *HyperTerminal* application. The following message box displays:

m. Click **Yes**. The following message box displays:



n. Click **No** to exit and close the *HyperTerminal* application.

o. Power off the maintenance terminal.

p. Disconnect the RS-232 modem cable from the switch and the maintenance terminal. Replace the protective cap over the maintenance port.

Was event code **433** reported?

NO **YES**

↓ An unrecoverable Ethernet fault (CTP failure) occurred. Because the CTP card is not a FRU, CTP failure requires replacing the switch.

Contact the next level of support.

MAP 0500: Fan and CTP Failure Analysis

This MAP describes fault isolation for the CTP (which is not a FRU) and fan FRUs. Failure indicators include:

- The amber LED on a fan illuminates.
- The amber emulated LED on a fan graphic at the **Hardware View** illuminates.
- A blinking red and yellow diamond (failed FRU indicator) displays at the **Product View** or **Hardware View**.
- An event code recorded at the switch *Event Log* or the Embedded Web Server event log.
- A `Failed` or `Not Installed` message associated with a fan at the Embedded Web Server interface.

1

Was an event code **300**, **301**, **302**, **303**, **304**, **305**, **306**, **307;** or **604**, **605**, **607**; or **800**, **801**, **802**, **805**, **806**, **807**, **810**, **811**, **812**, or **850** observed at the switch Event Log (HAFM server) or at the Embedded Web Server event log?

YES **NO**

↓ **Go to** step 3.

2

The following table lists event codes, brief explanations of the codes, and associated steps that describe fault isolation procedures.

Event Code	Explanation	Action
300	First cooling fan failed.	Go to step 8.
301	Second cooling fan failed.	Go to step 8.
302	Third cooling fan failed.	Go to step 8.
303	Fourth cooling fan failed.	Go to step 8.
304	Fifth cooling fan failed (does not apply to Edge Switch 2/32).	Go to step 8.
305	Sixth cooling fan failed (does not apply to Edge Switch 2/32).	Go to step 8.
306	First cooling fan in fan FRU assembly failed. (does not apply to Edge Switch 2/32)	Go to step 8.
307	Second cooling fan in fan FRU assembly failed. (does not apply to Edge Switch 2/32)	Go to step 8.
604	SBAR failure.	Go to step 14.
605	SBAR revision not supported.	Go to step 12.
800	High-temperature warning (port module sensor)	Go to step 8.
801	Critically hot temperature warning (port module thermal sensor)	Go to step 8.
802	Port module shutdown due to thermal violations.	Go to step 8.

Event Code	Explanation	Action
805	High-temperature warning (SBAR thermal sensor).	Go to step 8.
806	Critically hot temperature warning (SBAR thermal sensor).	Go to step 8.
807	SBAR shutdown due to thermal violation.	Go to step 8.
810	High temperature warning (CTP thermal sensor).	Go to step 8.
811	Critically hot temperature warning (CTP thermal sensor).	Go to step 8.
812	CTP shutdown due to thermal violation.	Go to step 8.
850	System shutdown due to CTP thermal violations.	Go to step 8.

3

Is remote fault isolation being performed at the switch or HAFM server?

YES **NO**

↓ Remote fault isolation is being performed through the Embedded Web Server interface. **Go to** step 6.

4

Does a blinking red and yellow diamond (failed FRU indicator) overlay a fan (cooling fan assembly) graphic at the **Hardware View**?

NO **YES**

↓ **Go to** step 8.

5

Does inspection of a fan indicate a failure? Indicators include:

- The amber LED at the upper left corner of a fan illuminates.
- The fan is not rotating.

NO **YES**

↓ **Go to** step 8.

The switch appears operational.

6

Does the Embedded Web Server interface appear operational?

YES **NO**

↓ Analysis for an Ethernet link, AC power distribution, or CTP failure is not described in this MAP. Go to "MAP 0000: Start MAP" on page 2-7. If this is the second time at this step, contact the next level of support.

7

Inspect the fan operational states at the Embedded Web Server interface.

a. At the **View** panel, click the **Component Properties** tab. The **View** panel (**Component Properties** tab) displays.

b. Inspect the **State** fields for Fan 0 through Fan 3.

Does the **State** field display a `Failed` message for any fan?

YES **NO**

↓ The switch appears operational.

8

A fan failed or is improperly installed.

a. Partially remove a fan from the chassis.

b. Reseat the fan in the chassis.

Does the fan appear to function?

NO **YES**

↓ The switch appears operational.

9

A fan failed and must be removed and replaced ("RRP: Cooling Fan" on page 4-6.

Does the fan appear to function?

NO **YES**

↓ The switch appears operational.

Contact the next level of support.

10

Have the customer inspect and verify that facility power is within specifications. These specifications are:

- One single-phase connection for each power supply.
- Input power between 120 and 230 Vac.
- Input current between 2 and 4 amps.
- Input frequency between 47 and 63 Hz.

Is facility power within specifications?

YES **NO**

↓ Ask the customer to correct the facility power problem. When facility power is corrected, verify switch temperature cools to within the operational limit.

11

Inspect the fans. Do one or more fans appear to rotate at insufficient angular velocity (failure pending)?

NO **YES**

↓ Remove and replace the affected fan ("RRP: Cooling Fan" on page 4-6 or. After fan replacement, verify switch temperature cools to within the operational limit.

A power supply problem is indicated. Go to "MAP 0100: Power Distribution Analysis" on page 2-26.

12

An SBAR is not recognized by switch firmware because the firmware version is not supported or the SBAR failed. Advise the customer of the problem and determine the correct firmware version to download from the HAFM server.

Download the firmware ("Download a Firmware Version to a Switch" on page 3-46). Perform the data collection procedure after the download.

Continue.

13

Did the firmware download solve the problem?

NO **YES**

↓ The switch appears operational.

14

The SBAR on the CTP card failed. Because the SBAR is not a FRU, SBAR failure requires replacing the switch.

Contact the next level of support.

MAP 0600: Port Failure and Link Incident Analysis

This MAP describes fault isolation for small form factor pluggable (SFP) transceivers and Fibre Channel link incidents. Failure indicators include:

- The amber LED adjacent to a Fibre Channel port illuminates.
- The amber emulated LED adjacent to a port graphic at the **Hardware View** illuminates.
- A blinking red and yellow diamond (failed FRU indicator) or yellow triangle (attention indicator) displays at the **Product View** or **Hardware View**.
- An event code recorded at the switch Event Log or the Embedded Web Server event log.
- A port failure message at the **Port Properties** dialog box or Embedded Web Server interface.
- A link incident message at the Link Incident Log or Port Properties.

1

Was an event code **080**, **440, 504**, **506**, **507**, **508**, **512**, **514**, or **604** observed at the switch Event Log (HAFM server) or at the Embedded Web Server event log?

NO **YES**

↓ **Go to** step 3.

2

Was an event code **581**, **582**, **583**, **584**, **585**, or **586** observed at the console of an OSI or FICON server attached to the switch reporting the problem.?

YES **NO**

↓ **Go to** step 4.

3

The following table lists event codes, brief explanations of the codes, and associated steps that describe fault isolation procedures.

Event Code	Explanation	Action
080	Unauthorized world wide name	Go to step 21
440	Embedded port hardware failure.	Go to step 11.
504	Port module failure — error threshold exceeded.	Go to step 11.
506	Fibre Channel port failure.	Go to step 11.
507	Loopback diagnostics port failure.	Go to step 12.
508	Fibre Channel port anomaly detected.	Go to step 12.
512	SFP nonfatal error.	Go to step 11.
514	SFP failure.	Go to step 11.
581	Implicit incident.	Go to step 32.
582	Bit-error threshold exceeded.	Go to step 34.
583	Loss of signal or loss of synchronization.	Go to step 32.
584	Not operational primitive sequence (NOS) received.	Go to step 32.
585	Primitive sequence timeout	Go to step 33.
586	Invalid primitive sequence received for link state.	Go to step 33.
604	SBAR failure.	Go to step 32.

4

Is fault isolation being performed at the switch or HAFM server?

YES **NO**

↓ Fault isolation is being performed through the Embedded Web Server interface. **Go to** step 35.

5

Is the amber LED adjacent to a Fibre Channel port illuminated, but not blinking?

NO **YES**

↓ **Go to** step 11.

6

Does a blinking red and yellow diamond (failed FRU indicator) overlay a port graphic at the **Hardware View**?

NO **YES**

↓ **Go to** step 11.

7

Did a Fibre Channel port fail a loopback test?

NO **YES**

↓ **Go to** step 12.

8

Perform link incident or failure analysis for the port.

Does a yellow triangle (attention indicator) overlay the port graphic at the **Hardware View**?

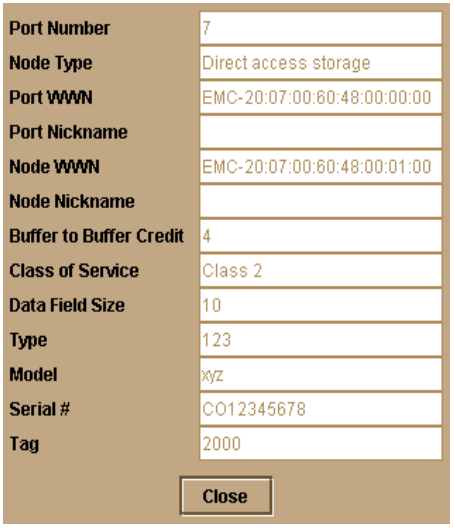
YES **NO**

↓ **Go to** step 10.

9

Inspect the port state and LED (green and amber) status.

a. At the **Hardware View**, click the port graphic. The **Port Properties** dialog box displays.



b. Inspect the **Operational State** field and the emulated green and amber LEDs adjacent to the port at the **Hardware View**.

c. The following table lists LED and port operational state combinations, and associated MAP 0600 (or other) steps that describe fault isolation procedures.

Operational State	Green LED	Amber LED	Action
Port Failure	Off	On	Go to step 11.
Offline	Off	Off	Go to step 14.
Not Operational	Off	Off	Go to step 14.
No Light	Off	Off	Go to step 14.
Testing	Off	Blinking	Internal loopback test in process.
Testing	On	Blinking	External loopback test in process.
Beaconing	Off or On	Blinking	Go to step 15.

Operational State	Green LED	Amber LED	Action
Inactive	Off	Off	See **Reason** Field of **Port Properties** dialog box.
Not Installed	Off	Off	The port optics are not installed or the feature that provides additional port function is not enabled.
Invalid attachment	On	Off	Go to step 16
Link Reset	On	Off	Go to step 24.
Link Incident	Off	Off	Go to step 25.
Segmented	On	Off	Go to MAP 0700.

10

A link incident may have occurred, but the LIN alerts option is not enabled for the port and the attention indicator does not display.

At the **Hardware View**, select **Link Incident Log** from the **Logs** menu on the navigation control panel. The Link Incident Log displays. If a link incident occurred, the affected port number is listed with one of the following messages.

```
Implicit incident.

Bit-error threshold exceeded.

Link failure — loss of signal or loss of synchronization.

Link failure — not-operational primitive sequence (NOS)
received.

Link failure — primitive sequence timeout.

Link failure — invalid primitive sequence received for the
current link state.
```

Is one of the listed messages displayed in the Link Incident Log?

NO **YES**

↓ **Go to** step 25.

11

A Fibre Channel port SFP failed and must be removed and replaced.

a. Determine the type of SFP to be removed and replaced. This procedure is concurrent and can be performed while switch power is on (RRP: SFP Transceiver on page 4-2).

b. Perform an external loopback test on the port SFP as part of FRU removal and replacement.

c. Perform the data collection procedure as part of FRU removal and replacement.

Did port SFP replacement solve the problem?

NO **YES**

↓ The switch appears operational.

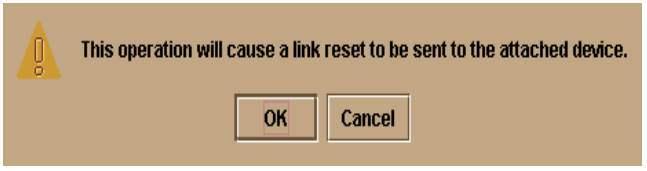
Contact the next level of support.

12

A Fibre Channel port SFP failed an internal or external loopback test.

a. Reset the failed port.

1. At the **Hardware View**, right-click the port. A pop-up menu displays.
2. Select **Reset Port**. A **Reset Port *n*** message box displays, where *n* is the port number (0 through 31).



3. Click **OK**. The port resets.

b. Perform an external loopback test for the port SFP.

Did resetting the port solve the problem?

NO **YES**

↓ The switch appears operational.

13

The port SFP may be improperly seated in the chassis. Partially remove and reseat the SFP, then perform an external loopback test for the SFP.

Did reseating the port SFP solve the problem?

NO **YES**

↓ The switch appears operational.

Go to step 11.

14

The fabric is initializing or a problem with the port-attached device is indicated as described by one of the following operational state messages:

- **`Offline`** — the port is blocked and transmitting the offline sequence (OLS) to the attached switch, or the port is unblocked and receiving the OLS, indicating the attached switch is set offline.
- **`Not Operational`** — the port is receiving the Fibre Channel not operational sequence (NOS), indicating the attached switch failed.
- **`No light (any port)`** — no signal (light) is received by the port. This is a normal condition when there is no cable attached to the port SFP or when the attached switch or fabric device is powered off.

Inform the customer an attached switch or fabric device is powered off, set offline, or failed.

15

Beaconing is enabled for the port.

a. Consult with the customer and next level of support to determine the reason port beaconing is enabled.

b. Disable port beaconing:

   1. At the **Hardware View**, right-click the port graphic. A pop-up menu displays.
   2. Click **Enable Beaconing**. The check mark disappears from the box adjacent to the option, and port beaconing is disabled.

Was port beaconing enabled because port failure or degradation was suspected?

YES **NO**

↓ The switch appears operational.

Go to step 4.

16

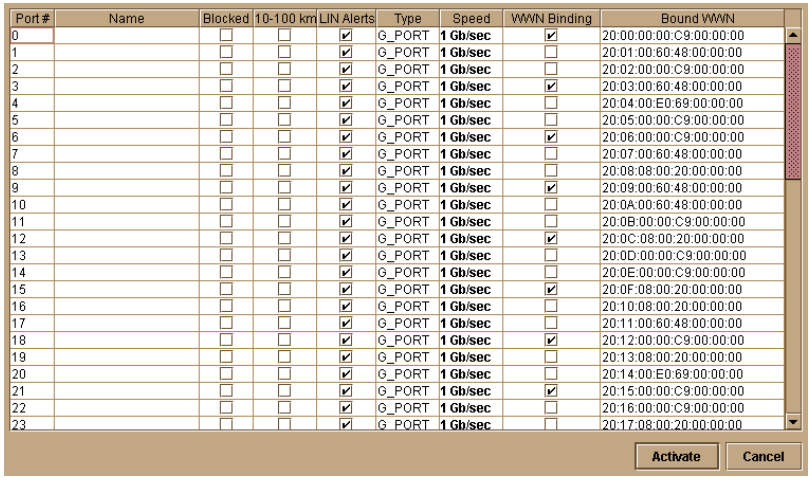
The port has an invalid attachment. The information in the **Port Properties** dialog box specifies the reason as listed in the following table.

Reason	Action
Unknown	Contact the next level of support.
ISL connection not allowed on this port.	Go to step 17.
Incompatible switch at other end of ISL.	Go to step 18.
External loopback adapter connected to the port.	Go to step 19.
N-Port connection not allowed on this port.	Go to step 17.
Non-HP switch at other end of the ISL.	Go to step 18.
Port binding violation — Unauthorized WWN.	Go to step 21.
Unresponsive node connected to port.	Go to step 22.

17

The port connection conflicts with the configured port type. Either an expansion port (E_Port) is incorrectly cabled to a Fibre Channel device or a fabric port (F_Port) is incorrectly cabled to a fabric element (director or switch).

a. At the HAFM server's **Hardware View**, click the **Configure** icon at the navigation control panel and select **Ports** from the **Configure** menu. The **Configure Ports** dialog box (open systems mode) displays.



Port #	Name	Blocked	10-100 km	LIN Alerts	Type	Speed	WWN Binding	Bound WWN
0		☐	☐	☑	G_PORT	1 Gb/sec	☑	20:00:00:00:C9:00:00:00
1		☐	☐	☑	G_PORT	1 Gb/sec	☐	20:01:00:60:48:00:00:00
2		☐	☐	☑	G_PORT	1 Gb/sec	☐	20:02:00:00:C9:00:00:00
3		☐	☐	☑	G_PORT	1 Gb/sec	☑	20:03:00:60:48:00:00:00
4		☐	☐	☑	G_PORT	1 Gb/sec	☐	20:04:00:E0:69:00:00:00
5		☐	☐	☑	G_PORT	1 Gb/sec	☐	20:05:00:00:C9:00:00:00
6		☐	☐	☑	G_PORT	1 Gb/sec	☑	20:06:00:00:C9:00:00:00
7		☐	☐	☑	G_PORT	1 Gb/sec	☐	20:07:00:60:48:00:00:00
8		☐	☐	☑	G_PORT	1 Gb/sec	☐	20:08:08:00:20:00:00:00
9		☐	☐	☑	G_PORT	1 Gb/sec	☑	20:09:00:60:48:00:00:00
10		☐	☐	☑	G_PORT	1 Gb/sec	☐	20:0A:00:60:48:00:00:00
11		☐	☐	☑	G_PORT	1 Gb/sec	☐	20:0B:00:00:C9:00:00:00
12		☐	☐	☑	G_PORT	1 Gb/sec	☑	20:0C:08:00:20:00:00:00
13		☐	☐	☑	G_PORT	1 Gb/sec	☐	20:0D:00:00:C9:00:00:00
14		☐	☐	☑	G_PORT	1 Gb/sec	☐	20:0E:00:00:C9:00:00:00
15		☐	☐	☑	G_PORT	1 Gb/sec	☑	20:0F:08:00:20:00:00:00
16		☐	☐	☑	G_PORT	1 Gb/sec	☐	20:10:08:00:20:00:00:00
17		☐	☐	☑	G_PORT	1 Gb/sec	☐	20:11:00:60:48:00:00:00
18		☐	☐	☑	G_PORT	1 Gb/sec	☑	20:12:00:00:C9:00:00:00
19		☐	☐	☑	G_PORT	1 Gb/sec	☐	20:13:08:00:20:00:00:00
20		☐	☐	☑	G_PORT	1 Gb/sec	☐	20:14:00:E0:69:00:00:00
21		☐	☐	☑	G_PORT	1 Gb/sec	☑	20:15:00:00:C9:00:00:00
22		☐	☐	☑	G_PORT	1 Gb/sec	☐	20:16:00:00:C9:00:00:00
23		☐	☐	☑	G_PORT	1 Gb/sec	☐	20:17:08:00:20:00:00:00

Activate Cancel

b. Use the vertical scroll bar as necessary to display the information row for the port indicating an invalid attachment.

c. Select (click) the **Type** field and configure the port from the list box as follows:

- Select **F_Port** (fabric port) if the port is cabled to a device (node).
- Select **E_Port** (expansion port) if the port is cabled to a fabric element (director or switch) to form an ISL.

d. Click the **Activate** button to save the configuration information and close the dialog box.

Did reconfiguring the port type solve the problem?

NO **YES**

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

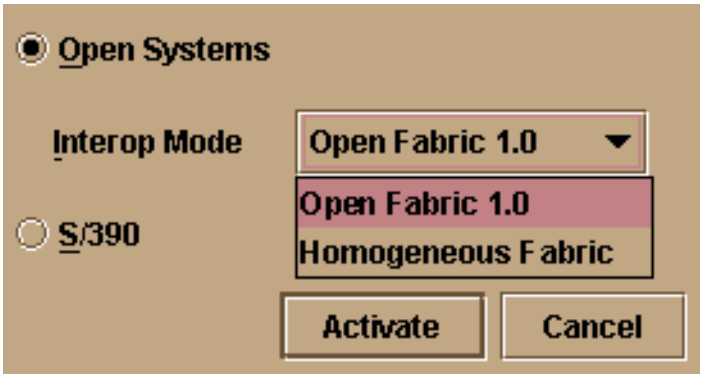
18

The switch is configured for Open Fabric mode and the switch at the other end of the ISL is an HP director or switch configured for Homogeneous mode. Or the switch is connected to a non-HP switch and interop mode is set to Homogeneous fabric mode.

Configure the switch operating mode:

a. Ensure the switch is set offline. For instructions, refer to "Set Offline State" on page 3-38 and return here.

b. At the **Hardware View** for the selected switch, click the **Configure** icon at the navigation control panel and select **Operating Mode** from the **Configure** menu. The **Configure Operating Mode** dialog box displays.



c. Select the operating mode as follows:

— Select the **Open Systems** radio button to set the switch to open systems operating mode, then select **Homogeneous Fabric** or **Open Fabric 1.0** from the **Interop Mode** list box.

Select **Homogeneous Fabric** if the switch is fabric-attached only to other HP switches that are also operating in homogeneous fabric mode. Select **Open Fabric 1.0** if the fabric contains HP switches and other open-fabric compliant switches.

d. Click the **Activate** button to save the selection and close the dialog box.

Did configuring the operating mode solve the problem?

NO **YES**

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

19

A loopback (wrap) plug is connected to the port and there is no diagnostic test running. Is a loopback plug in the port receptacle?

YES **NO**

↓ Contact the next level of support. **Exit MAP.**

20

Remove the loopback plug from the port receptacle. If directed by the customer, connect a fiber-optic jumper cable attaching a device to the switch.

- If the port is operational and a device is not attached, both LEDs adjacent to the port extinguish and the port state is No Light.
- If the port is operational and a device is attached, the green LED illuminates, the amber LED extinguishes, and the port state is Online.

Did removing the loopback plug solve the problem?

NO **YES**

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**

21

The WWN entered to configure port binding for this port is not valid or a nickname was used that was not configured for the attached device in the Product Manager.

Open the **Node List View** from the **Hardware View**, and select **Node List** from the **View** menu on the navigation control panel. Note the **Port WWN** column.

The Port WWN is the eight-byte (16-digit) worldwide name (WWN) assigned to the port or Fibre Channel interface installed on the attached device.

— If a nickname is not assigned to the WWN, the WWN is prefixed by the device manufacturer's name.

— If a nickname is assigned to the WWN, the nickname displays in place of the WWN.

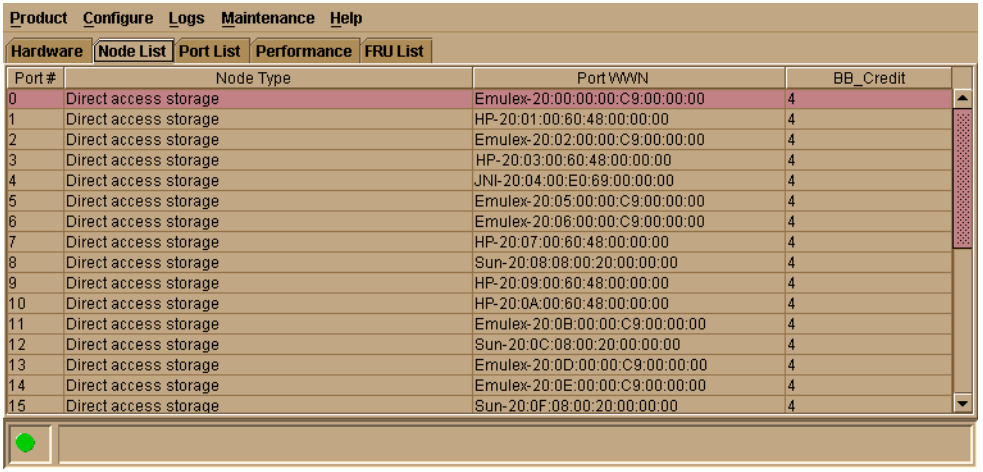
The Bound WWN must be in the form of the raw WWN format (xx:xx:xx:xx:xx:xx:xx:xx) or must be a valid nickname.

Did configuring the WWN or nickname solve the problem?

NO **YES**

↓ The switch appears operational. **Exit MAP.**

Contact the next level of support. **Exit MAP.**


Product Configure Logs Maintenance Help
Hardware Node List Port List Performance FRU List
Port # Node Type Port WWN BB_Credit
0 Direct access storage Emulex-20:00:00:00:C9:00:00:00 4
1 Direct access storage HP-20:01:00:60:48:00:00:00 4
2 Direct access storage Emulex-20:02:00:00:C9:00:00:00 4
3 Direct access storage HP-20:03:00:60:48:00:00:00 4
4 Direct access storage JNI-20:04:00:E0:69:00:00:00 4
5 Direct access storage Emulex-20:05:00:00:C9:00:00:00 4
6 Direct access storage Emulex-20:06:00:00:C9:00:00:00 4
7 Direct access storage HP-20:07:00:60:48:00:00:00 4
8 Direct access storage Sun-20:08:08:00:20:00:00:00 4
9 Direct access storage HP-20:09:00:60:48:00:00:00 4
10 Direct access storage HP-20:0A:00:60:48:00:00:00 4
11 Direct access storage Emulex-20:0B:00:00:C9:00:00:00 4
12 Direct access storage Sun-20:0C:08:00:20:00:00:00 4
13 Direct access storage Emulex-20:0D:00:00:C9:00:00:00 4
14 Direct access storage Emulex-20:0E:00:00:C9:00:00:00 4
15 Direct access storage Sun-20:0F:08:00:20:00:00:00 4

22

Clean the fiber-optic connectors on the cable.

a. Notify the customer the port will be blocked. Ensure the customer's system administrator stops Fibre Channel frame traffic through the port and sets the attached device offline.

b. Block the port. Refer to "Block a Port" on page 3-39 for instructions.

c. Disconnect both ends of the fiber-optic cable.

d. Clean the fiber-optic connectors. Refer to "Clean Fiber-Optic Components" on page 3-33 for instructions.

e. Reconnect the fiber-optic cable.

f. Unblock the port. Refer to "Unblock a Port" on page 3-40 for instructions.

g. Monitor port operation for approximately five minutes.

Did the link incident recur?

YES **NO**

↓ The Fibre Channel link and switch appear operational.
Exit MAP.

23

Inspect and service the host bus adapters (HBAs), as necessary.

Did service of the HBAs solve the problem?

NO **YES**

↓ **Exit MAP.**

Contact the next level of support. **Exit MAP.**

24

The switch and attached fabric device are performing a Fibre Channel link reset. This is a transient state. Wait approximately 30 seconds and inspect port state and LED behavior.

Did the link recover and resume operation?

NO **YES**

↓ The Fibre Channel link and switch appear operational.

Go to step 4.

25

A link incident message appeared in the Link Incident Log or in the **Link Incident** field the **Port Properties** dialog box.

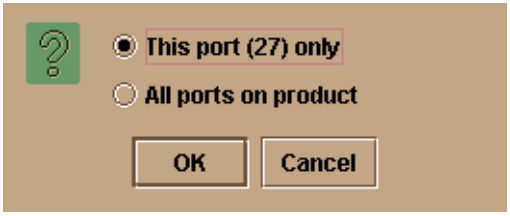
Clear the link incident for the port.

a. At the **Hardware View**, right-click the port graphic. A pop-up menu displays.

b. Select **Clear Link Incident Alert(s)**. The **Clear Link Incident Alert(s)** dialog box displays.

c. Select the **This port (*n*) only** radio button (where *n* is the port number) and click **OK**. The link incident clears.

d. Monitor port operation for approximately five minutes.



Did the link incident recur?

YES **NO**

↓ The problem is transient. The Fibre Channel link and the switch appear operational.

26

Inspect the fiber-optic jumper cable attached to the port and ensure the cable is not bent and connectors are not damaged. If the cable is bent or connectors are damaged:

a. Notify the customer the port will be blocked. Ensure the customer system administrator stops Fibre Channel frame traffic through the port and sets the attached switch or device offline.

b. Block the port ("Block a Port" on page 3-39).

c. Remove and replace the fiber-optic jumper cable.

d. Unblock the port ("Unblock a Port" on page 3-40).

Was a corrective action performed?

YES **NO**

↓ **Go to** step 28.

27

Monitor port operation for approximately five minutes.

Did the link incident recur?

YES **NO**

↓ The Fibre Channel link and switch appear operational.

28

Clean fiber-optic connectors on the jumper cable.

a. Notify the customer the port will be blocked. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port and sets the attached switch or device offline.

b. Block the port ("Block a Port" on page 3-39).

c. Disconnect both ends of the fiber-optic jumper cable.

d. Clean the fiber-optic connectors ("Clean Fiber-Optic Components" on page 3-33)

e. Reconnect the fiber-optic jumper cable.

f. Unblock the port ("Unblock a Port" on page 3-40).

g. Monitor port operation for approximately five minutes.

Did the link incident recur?

YES **NO**

↓ The Fibre Channel link and switch appear operational.

29

Disconnect the fiber-optic jumper cable from the port and connect the cable to a spare port.

Is a link incident reported at the new port?

YES **NO**

↓ **Go to** step 31.

30

The attached device is causing the recurrent link incident. Notify the customer of the problem and have the system administrator:

a. Inspect and verify operation of the attached device.

b. Repair the attached device if a failure is indicated.

c. Monitor port operation for approximately five minutes.

Did the link incident recur?

YES **NO**

↓ The attached device, Fibre Channel link, and switch appear operational.

Contact the next level of support

31

The switch port reporting the problem is causing the recurrent link incident. The recurring link incident indicates port degradation and a possible pending failure. **Go to** step 11.

32

An implicit incident error (event code **581**), loss of signal or loss of synchronization (event code **583**), not operational primitive sequence (NOS) received (event code **584**), or SBAR failure (event code **604**) caused the switch to fault.

Perform the data collection procedure and return the Zip disk to HP for analysis.

33

The switch primitive sequence timed out (event code **585**) or an invalid primitive sequence was received for link state (event code **586**). Either error causes the switch to automatically reinitialize the fabric. Attached devices may momentarily logout, login, and resume operation.

If the problem persists, an attached device may be marginally operating and causing the error condition. Inform the customer of the problem.

34

A port was bypassed because a bit-error threshold was exceeded (event code **582**).

If the problem persists, the attached device may be marginally operating and causing the error condition. Inform the customer of the problem.

35

Does the Embedded Web Server interface appear operational?

YES **NO**

↓ Analysis for an Ethernet link, AC power distribution, or CTP failure is not described in this MAP. Go to "MAP 0000: Start MAP**" on page 2-7**. If this is the second time at this step, contact the next level of support.

36

Inspect port operational states at the Embedded Web Server interface.

a. At the **View** panel, click the **Port Properties** tab. The **View** panel (**Port Properties** tab) displays.

b. Inspect the **Operational State** field.

c. At the **View** panel (**Port Properties** tab) click the first port (1).

d. Inspect the **Operational State** field.

e. At the **View** panel (**Port Properties** tab) sequentially click the remaining ports. Inspect the **Operational State** field for each port.

Does the **Operational State** field display a `Segmented` message for a port?

NO **YES**

↓ Port segmentation is indicated. Go to "MAP 0700: Fabric, ISL, and Segmented Port Problem Determination" on page 2-79.

37

Does the **Operational State** field display a `Port Failure` message for any port?

NO **YES**

↓ A port SFP failure is indicated. **Go to** step 11.

The switch appears operational.

MAP 0700: Fabric, ISL, and Segmented Port Problem Determination

This MAP describes isolation of fabric logout, interswitch link (ISL), and port segmentation problems. Failure indicators include:

- An event code recorded at the switch *Event Log* or the Embedded Web Server event log.
- A segmentation reason associated with the port at the Embedded Web Server interface.
- A yellow triangle (attention indicator) displays at the **Product View** or **Hardware View**.
- A link incident message recorded in the **Link Incident Log** or **Port Properties** dialog box.

1

Was an event code **011**, **021**, **051**, **052, 061**, **062**, **070**, **071**, or **072,** observed at the switch Event Log (HAFM server) or at the Embedded Web Server event log?

YES **NO**

↓ **Go to** step 3.

2

The following table lists event codes, brief explanations of the codes, and associated steps that describe fault isolation procedures.

Event Code	Explanation	Action
011	Login server database invalid.	Go to step 7.
021	Name server database invalid.	Go to step 7.
051	Management server database invalid.	Go to step 7.
052	Management server internal error.	Go to step 7.
061	Fabric controller database invalid.	Go to step 7.
062	Maximum interswitch hop count exceeded.	Go to step 8.
070	E_Port is segmented.	Go to step 9.
071	Switch is isolated.	Go to step 9.
072	E_Port connected to an unsupported switch.	Go to step 10.

3

Is fault isolation being performed at the HAFM server?

YES **NO**

↓ Fault isolation is being performed through the Embedded Web Server interface. **Go to** step 17.

4

Does a yellow triangle (attention indicator) overlay the port graphic at the **Hardware View**?

YES **NO**

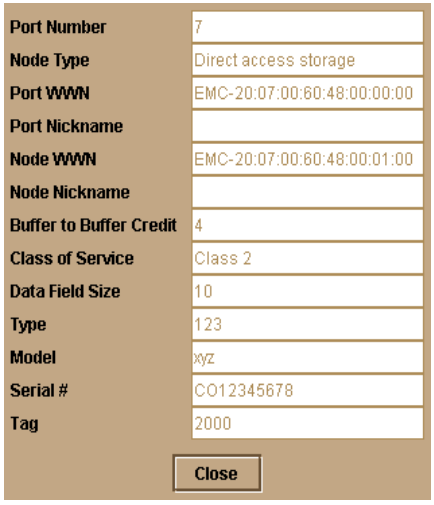
↓ The problem is transient and the switch-to-fabric device connection appears operational.

5

Inspect the port state and LED status for the port.

a. At the **Hardware View**, click the port graphic. The **Port Properties** dialog box displays.

b. Inspect the **Operational State** field.



Does the **Operational State** field indicate `Segmented E_Port`?

YES **NO**

↓ Analysis for a port failure or other link incident is not described in this MAP. Go to "MAP 0600: Port Failure and Link Incident Analysis" on page 2-63.

6

Inspect the **Reason** field at the **Port Properties** dialog box. The following table lists port segmentation reasons and associated steps that describe fault isolation procedures.

Segmentation Reason	Action
Incompatible operating parameters.	Go to step 11.
Duplicate domain IDs.	Go to step 12.
Incompatible zoning configurations.	Go to step 13.
Build fabric protocol error.	Go to step 14.
No principal switch.	Go to step 19.
No response from attached switch.	Go to step 16.

7

As indicated by an event code **052,** a minor internal operating error was detected by the management server subsystem. The error caused management server databases to be re-initialized to an empty state. As a result, a disruptive server logout and login occurred for all attached devices. All attached devices resume operation after management server login.

Perform the data collection procedure and return the Zip disk to HP for analysis.

8

As indicated by an event code **062**, the fabric controller software detected a path within the connected multi-switch fabric that traverses more than seven interswitch links (ISLs or hops). Fibre Channel frames may persist in the fabric longer than timeout values allow.

Advise the customer of the problem and work with the system administrator to reconfigure the fabric so the path between any two switches does not traverse more than seven hops.

Did fabric reconfiguration solve the problem?

NO YES

↓ The switch and connected multi-switch fabric appear operational.

Contact the next level of support.

9

A **070** event code indicates the E_Port detected an incompatibility with an attached switch and prevented the switches from forming a multi-switch fabric. A segmented E_port cannot transmit Class 2 or Class 3 Fibre Channel traffic.

A **071** event code indicates the switch is isolated from all switches in a multi-switch fabric, and is accompanied by a **070** event code for the segmented E_Port. The **071** event code is resolved when all **070** events are corrected.

Obtain supplementary event data for the **070** event code.

a. At the switch Event Log or the Embedded Web Server event log, record the first four bytes (0 through 3) of event data.

b. Examine the first five bytes (0 through 4) of event data.

c. Byte 0 specifies the port number (00 through 31) of the segmented E_port. Byte 4 specifies the segmentation reason as listed in the following table.

Byte 3	Segmentation Reason	Action
01	Incompatible operating parameters.	Go to step 11.
02	Duplicate domain IDs.	Go to step 12.
03	Incompatible zoning configurations.	Go to step 13.
04	Build fabric protocol error.	Go to step 14.
05	No principal switch.	Go to step 19.
06	No response from attached switch (Hello Timeout).	Go to step 16.

10

As indicated by an event code **072**, the switch E_Port is connected to an unsupported switch.

Advise the customer of the problem and disconnect the interswitch link to the unsupported switch.

11

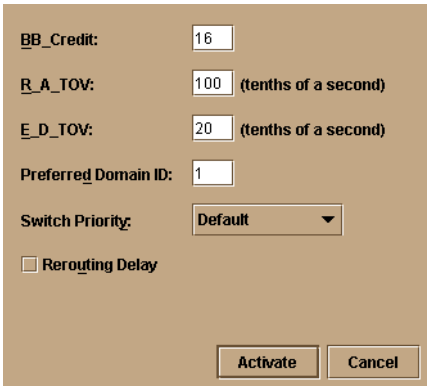
The switch E_Port segmented because the error detect time-out value (*E_D_TOV*) or resource allocation time-out value (*R_A_TOV*) is incompatible with the attached fabric element.

a. Contact HP customer support or engineering personnel to determine the recommended *E_D_TOV* and *R_A_TOV* values for the switches.

b. Notify the customer that both switches will be set offline. Ensure the system administrator stops Fibre Channel frame traffic through the switches and sets attached devices offline.

c. Set both switches offline ("Set Offline State" on page 3-38).

d. At the **Hardware View** for the switch, select **Operating Parameters** from the **Configure** menu on the navigation control panel. The **Configure Operating Parameters** dialog box displays.



e. Type the recommended *E_D_TOV* and *R_A_TOV* values, then click **Activate**.

f. Repeat steps d and e at the **Hardware View** for the switch attached to the segmented switch. Use the same *E_D_TOV* and *R_A_TOV* values.

g. Set both switches online ("Set Online State" on page 3-37).

Did the operating parameter change solve the problem and did both switches join through the ISL to form a fabric?

NO **YES**

↓ The switches, associated ISL, and multi-switch fabric appear operational.

Contact the next level of support.

12

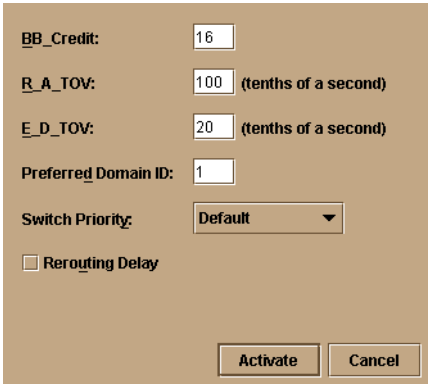
The switch E_Port segmented because two fabric elements have duplicate domain IDs.

a. Work with the system administrator to determine the desired domain ID (1 through 31 inclusive) for both switches.

b. Notify the customer that both switches will be set offline. Ensure the system administrator quiesces Fibre Channel frame traffic through the switches and sets attached devices offline.

c. Set both switches offline ("Set Offline State" on page 3-38).

d. At the **Hardware View** for the switch, select **Operating Parameters** from the **Configure** menu on the navigation control panel. The **Configure Operating Parameters** dialog box displays.



e. Type the customer-determined preferred domain ID value, then click **Activate**.

f. Repeat steps d and e at the **Hardware View** for the switch attached to the segmented E-Port (second switch). Use a different preferred domain ID value.

g. Set both switches online ("Set Online State" on page 3-37).

Did the domain ID change solve the problem and did both switches join through the ISL to form a fabric?

NO **YES**

↓ The switches, associated ISL, and multi-switch fabric appear operational.

Contact the next level of support.

13

The switch E_Port segmented because two switches have incompatible zoning configurations. An identical zone name is recognized in the active zone set for both switches, but the zones contain different members.

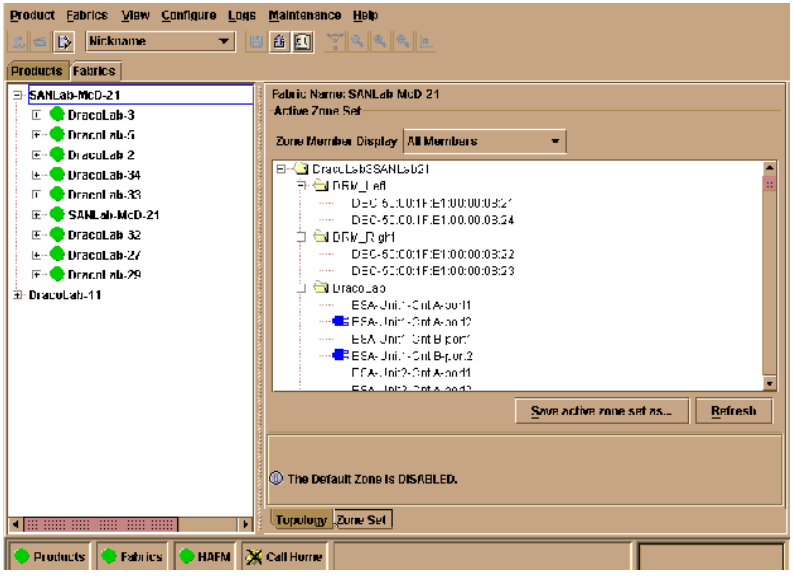
a. Work with the system administrator to determine the desired zone name change for the one of the affected switches.Zone names must conform to the following rules:

- The name must be 64 characters or fewer in length.
- The first character must be a letter (a through z), upper or lower case.
- Other characters are alphanumeric (a through z or 0 through 9), dollar sign ($), hyphen (-), caret (^), or underscore (_).

b. Close the *Product Manager* application for the switch (**Hardware View**). The main HAFM window, or **Product View** (still active) displays.

c. Select the **Fabrics** tab from the **View** menu. The **Fabrics View** displays with the default **Topology** tab active.

d. Select the **Zone Set** tab at the bottom of the window. The **Zone Set** tab becomes active and displays the active zone set.



e. Inspect zone names in the active zone set to determine the incompatible name.

f. Modify the incompatible zone name as directed by the customer:

1. At the navigation control panel, select **Zone Sets** from the **Configure** menu. The **Zone Sets** dialog box displays.
2. Select (highlight) the active zone set name, then select **Modify** from the **Actions** icon on the dialog box. The **Modify Zone Set** dialog box displays.
3. Select (highlight) the zone name to be modified (and later deleted) at the **Zone Library** list, then select **Copy Zone** from the **Actions** icon on the dialog box. The **Copy Zone** dialog box displays.
4. Type the new zone name (specified by the customer) and click **OK**. The new zone name displays in the **Zone Library** list. The new zone contains the same members as the copied zone.

5. Select (highlight) the new zone name and drag (holding the left mouse button) the name to the **Zones in Set** list.
6. At the **Zones in Set** list, select (highlight) the zone name to be deleted, then drag (holding the left mouse button) the name off the **Modify Zone Set** dialog box.
7. At the **Modify Zone Set** dialog box, click **Save Zone Set**. The zone set (with the new zone name) is saved and the dialog box closes.
8. At the **Zone Sets** dialog box, select (highlight) the active zone set name, then select **Activate from the Actions** icon on the dialog box. The **Activate Zone Set** dialog box displays.
9. Click **Start**. The status message changes to `Activate zone set complete`. Click **Close** to close the dialog box.
10. Click **Close** to close the **Zone Sets** dialog box and return to the **Zoning Set View** with the modified active zone set.

Did the zone name change solve the problem and did both switches join through the ISL to form a fabric?

NO **YES**

↓ The switches, associated ISL, and multi-switch fabric appear operational.

Contact the next level of support.

14

The switch E_Port segmented because a build fabric protocol error was detected.

a. Disconnect the fiber-optic jumper cable from the segmented E_Port.
b. Reconnect the cable to the same port.

Did reconnecting the cable solve the problem and did both switches join through the ISL to form a fabric?

NO **YES**

↓ The switches, associated ISL, and multi-switch fabric appear operational.

15

Initial program load (IPL) the switch (Reset or IPL the Switch on page -35).

Did the IPL solve the problem and did both switches join through the ISL to form a fabric?

NO **YES**

↓ The switches, associated ISL, and multi-switch fabric appear operational.

Contact the next level of support.

16

The switch E_Port segmented because a response to a verification check indicates the attached switch is not operational.

a. Perform the data collection procedure for the switch and return the Zip disk to HP for analysis.

b. Go to "MAP 0000: Start MAP" on page 2-7 and perform fault isolation for the failed switch.

17

Does the Embedded Web Server interface appear operational?

YES **NO**

↓ Analysis for an Ethernet link, AC power distribution, or CTP failure is not described in this MAP. Go to "MAP 0000: Start MAP" on page 2-7. If this is the second time at this step, contact the next level of support.

18

Inspect the Fibre Channel port segmentation reason at the Embedded Web Server interface.

a. At the **View** panel, click the **Port Properties** tab. The **View** panel (**Port Properties** tab) displays.

b. Click the port number (0 through 31) of the segmented port.

c. Inspect the **Reason** field for the port.

Is the **Reason** field blank or does it display an `N/A` message?

NO **YES**

↓ The switch ISL appears operational.

The **Reason** field displays a reason message. The following table lists segmentation reasons and associated steps that describe fault isolation procedures.

Segmentation Reason	Action
`Incompatible operating parameters.`	Go to step 11.
`Duplicate domain IDs.`	Go to step 12.
`Incompatible zoning configurations.`	Go to step 13.

Segmentation Reason	Action
Build fabric protocol error.	Go to step 14.
No principal switch.	Go to step 19.
No response from attached switch.	Go to step 16.

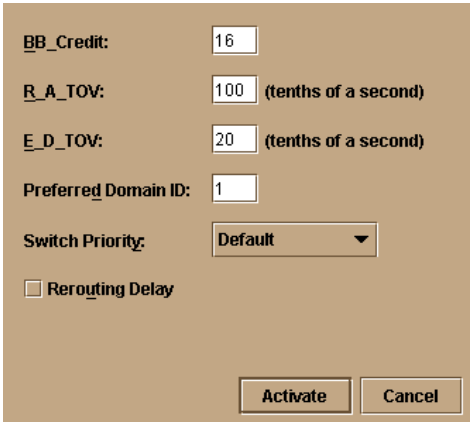
19

A switch E_Port segmented because no switch in the fabric is capable of becoming the principal switch.

a. Notify the customer that the switch will be set offline. Ensure the system administrator quiesces Fibre Channel frame traffic through the switch and sets attached devices offline.

b. Set the switch offline ("Set Offline State" on page 3-38)

c. At the **Hardware View** or **Port Card View** for the switch, select **Operating Parameters** from the **Configure** icon on the navigation control panel. The **Configure Operating Parameters** dialog box displays.



d. At the **Switch Priority** field, select **Principal**, **Never Principal**, or **Default** (the default setting is **Default**). Then click **Activate**.

e. Set the switch online ("Set Online State" on page 3-37)

Did the switch priority change solve the problem and did both switches join through the ISL to form a fabric?

NO **YES**

↓ The switches, associated ISL, and multi-switch fabric appear operational.

C**ontact the next level of support.**

MAP 0800: Console PC Problem Determination

This MAP describes isolation of hardware-related problems with the HAFM server platform. Although this MAP provides high-level fault isolation instructions, refer to the documentation provided with the PC for detailed problem determination and resolution.

1

At the HAFM server, close the *HAFM* application.

a. At the navigation control panel of the **Product View**, select **Exit** from the **Logout/Exit** icon. The *HAFM* application closes.

b. Close any other applications that are running.

Continue.

2

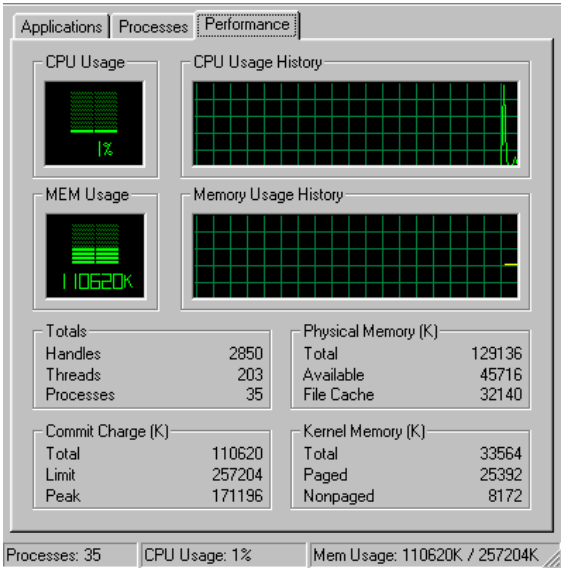
Inspect the available random access memory (RAM). The computer must have a minimum of 64 megabytes (MB) of memory to run the Windows operating system and *HAFM* application.

a. Right-click anywhere in the Windows task bar at the bottom of the desktop. A pop-up menu displays.

b. Select **Task Manager**. The **Windows Task Manager** dialog box displays with the **Performance** page open.

c. At the **Physical Memory (K)** portion of the dialog box, inspect the total amount of physical memory.

d. Close the dialog box by clicking **Close** at the upper right corner of the window.



Does the computer have sufficient memory?

YES **NO**

↓ A memory upgrade is required. Inform the customer of the problem and contact the next level of support.

3

Reboot the HAFM server PC and perform system diagnostics.

a. Click the **Windows Start** button. The **Windows Workstation** menu displays.

b. At the **Windows Workstation** menu, select **Shut Down**. The **Shut Down Windows** dialog box displays.

c. At the **Shut Down Windows** dialog box, select **Shut down the Computer** and click **Yes** to power off the PC.

d. Wait approximately 30 seconds and power on the PC. After POSTs complete, the **Begin Logon** dialog box displays.

e. Simultaneously press **Ctrl**, **Alt**, and **Delete** to display the **Logon Information** dialog box. Type a user name and password (obtained in "MAP 0000: Start MAP" on page 2-7) and click **OK**. The Windows desktop displays.

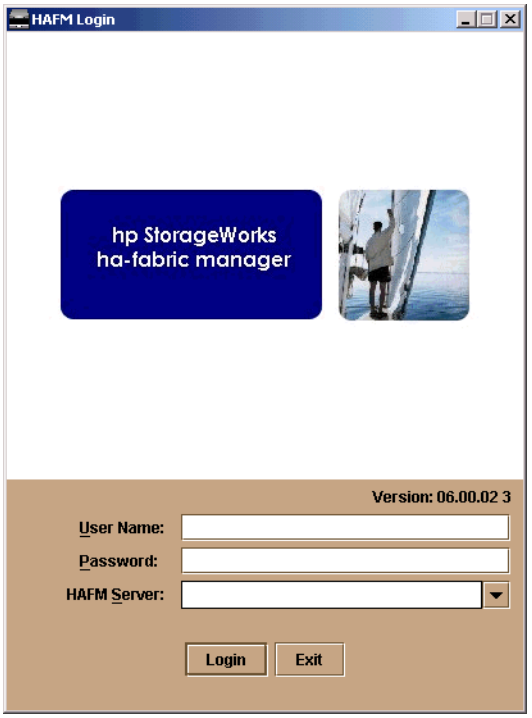
Did POSTs detect a problem?

NO **YES**

↓ A computer hardware problem exists. Refer to the supporting documentation shipped with the PC for instructions on resolving the problem.

4

After rebooting the PC, the *HAFM* application starts and the **HAFM Login** dialog box displays.



Did the **HAFM Login** dialog box display?

YES **NO**

↓ **Go to** step 6.

5

At the **HAFM Login** dialog box, type a user name, password, and HAFM server name (obtained in "MAP 0000: Start MAP" on page 2-7, and all are case sensitive), and click **Login**. The application opens and the **Product View** displays.

Did the **Product View** display and does the *HAFM* application appear operational?

NO **YES**

↓ The PC appears operational.

6

Perform one of the following:

- If the PC has standalone diagnostic test programs resident on the hard drive, perform the diagnostics. Refer to supporting documentation shipped with the PC for instructions.
- If the PC does not have standalone diagnostic test programs resident on fixed disk, **go to** step 7.

Did diagnostic test programs detect a problem?

NO **YES**

↓ Refer to the supporting documentation shipped with the PC for instructions to resolve the problem.

7

Reboot the HAFM server PC.

a. Click the **Windows Start** button. The **Windows Workstation** menu displays.

b. At the **Windows Workstation** menu, select **Shut Down**. The **Shut Down Windows** dialog box displays.

c. At the **Shut Down Windows** dialog box, select **Shut down the Computer** and click **Yes** to power off the PC.

d. Wait approximately 30 seconds and power on the PC. After POSTs complete, the **Begin Logon** dialog box displays.

e. Simultaneously press **Ctrl**, **Alt**, and **Delete** to display the **Logon Information** dialog box. Type a user name and password (obtained in "MAP 0000: Start MAP" on page 2-7) and click **OK**. The *HAFM* application starts and the **HAFM Login** dialog box displays.

f. At the **HAFM Login** dialog box, type a user name, password, and HAFM server name (obtained in "MAP 0000: Start MAP" on page 2-7, and all are case sensitive), and click **Login**. The application opens and the **Product View** displays.

Did the **Product View** display and does the *HAFM* application appear operational?

NO **YES**

↓ The PC appears operational.

8

Re-install the *HAFM* application ("Install or Upgrade Software" on page 2-51).

Did the *HAFM* application install and open successfully?

NO **YES**

↓ The PC appears operational.

9

Advise the customer and next level of support that the PC hard drive should be formatted. If the customer and support personnel do not concur, **go to** step 10.

a. Format the PC hard drive. Refer to supporting documentation shipped with the PC for instructions.

b. Install the Windows operating system and *HAFM* application.

Did the PC hard drive format, and did the operating system and *HAFM* application install and open successfully?

NO **YES**

↓ The PC appears operational.

10

Additional analysis for the failure is not described in this MAP. **Contact the next level of support.**

3

Repair Information

This chapter describes the repair and repair-related procedures for the HP StorageWorks Edge Switch 2/32, and associated field-replaceable units (FRUs). These procedures are described:

- Obtaining log information at the HP StorageWorks High Availability Fabric Manager (HAFM) server.
- Displaying and using HAFM server views.
- Obtaining and interpreting port diagnostic and performance data, and performing port diagnostic loopback tests.
- Swapping ports (S/390 mode only).
- Collecting maintenance data.
- Cleaning fiber-optic components.
- Powering the switch on and off.
- Performing an initial program load (IPL).
- Setting the switch online or offline.
- Blocking or unblocking Fibre Channel ports.
- Managing firmware versions.
- Managing configuration data.
- Installing or upgrading software.

Do not perform repairs until a failure is isolated to a FRU. If fault isolation was not performed, refer to "MAP 0000: Start MAP" on page 2-7.

Factory Defaults

Table 3–1 lists the defaults for the passwords, and IP, subnet, and gateway addresses.

Table 3–1: Factory-Set Defaults

Item	Default
Customer password	password
Maintenance password	level-2
IP address	10.1.1.10
Subnet mask	255.0.0.0
Gateway address	0.0.0.0

Procedural Notes

NOTE: HAFM and Product Manager screens in this manual may not match the screens on your server and workstation. The title bars have been removed and the fields may contain data that does not match the data seen on your system.

The following procedural notes are referenced in applicable repair procedures. The notes do not necessarily apply to all procedures in the chapter.

1. Before performing a repair procedure, read the procedure carefully and thoroughly to familiarize yourself with the information and reduce the possibility of problems or customer down time.
2. When performing procedures described in this chapter, heed all **WARNING** and **CAUTION** statements, and other statements listed in the preface of this manual.
3. After completing steps of a detailed procedure that is referenced from another procedure, return to the initial (referencing) procedure and continue to the next step of that procedure.

1. After replacing a FRU, extinguish the System Error light-emitting diode (LED) on the front of the switch.

Using Log Information

The HAFM and switch Product Manager provide access to ten logs that provide information for administration, operation, and maintenance personnel. Each log stores up to 1,000 entries. The most recent entry displays at the top of a log. If a log is full, a new entry overwrites the oldest entry.

Five logs are accessed through the *HAFM* application:

- HAFM Audit Log.
- HAFM Event Log.
- Session Log.
- Product Status Log.
- Fabric Log

Five logs are accessed through the *Product Manager* application:

- Switch Audit Log.
- Switch Event Log.
- Hardware Log.
- Link Incident Log.
- Threshold Alert Log.

HAFM Audit Log

The HAFM audit log displays a history of user actions performed through the *HAFM* application. This information is useful for system administrators and users. To open the HAFM audit log, select **Audit Log** from the **Logs** menu on the navigation control panel.

For a description of the HAFM audit log and an explanation of button functions at the bottom of the log window, refer to the *hp StorageWorks High Availability Fabric Manager user guide*.

HAFM Event Log

The HAFM Event Log (Figure 3–1) displays events or error conditions recorded by the *HAFM Services* application. Entries reflect the status of the application and managed switches.

Information associated with a call-home failure is intended for maintenance personnel to fault isolate the problem (modem failure, no dial tone, etc.), while information provided in all other entries is generally intended for use by third-level support personnel to isolate more significant problems.

To open the HAFM Event Log, select **Event Log** from the **Logs** menu on the navigation control panel.

Figure 3–1: HAFM Event Log

The event log contains the following columns:

- **Date/Time —** the date and time the event was reported to the HAFM server.
- **Event —** an event number and brief description of the event. Include both the event number and description when reporting an event to third-level customer support.
- **Product —** the product associated with the event. Some events are associated with the *HAFM Services* application, while others are associated with a specific instance of the *HAFM* application. In the latter case, the product and configured name (or internet protocol (IP) address) associated with the instance are displayed.
- **Qualifier —** this column provides an event qualifier for use by engineering personnel. Include this number when reporting an event to third-level customer support.
- **Data —** additional event data for fault isolating a problem. Use the information when fault isolating a call-home problem, or include the information when reporting an event to third-level customer support.

Session Log

The Session Log displays a session (login and logout) history for the HAFM server, including the date and time, user name, and network address of each session. This information is useful for system administrators and users. To open the Session Log, select **Session Log** from the **Logs** menu on the navigation control panel.

For a description of the Session Log and an explanation of button functions at the bottom of the log window, refer to the *hp StorageWorks High Availability Fabric Manager user guide*.

Product Status Log

The Product Status Log (Figure 3–2) records an entry when the status of a switch changes. The log reflects the previous status and current status of the switch, and indicates the instance of a switch *Product Manager* application that should be opened to investigate a problem. The information is useful to maintenance personnel for fault isolation and repair verification.

To open the Product Status Log, select **Product Status Log** from the **Logs** menu on the navigation control panel.

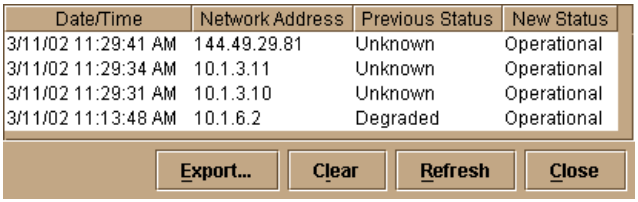


Figure 3–2: Product Status Log

The log contains the following columns:

- **Date/Time —** the date and time the switch status change occurred.
- **Network Address —** the IP address or configured name of the switch. This address or name corresponds to the address or name displayed under the switch icon at the **Product View**.
- **Previous Status —** the status of the switch prior to the reported status change (Operational, Degraded, Failed, or Unknown). An Unknown status indicates the *HAFM* application cannot communicate with the switch.
- **New Status —** the status of the switch after to the reported status change (Operational, Degraded, Failed, or Unknown).

Fabric Log

The Fabric Log reflects the time and nature of significant changes in the managed fabric.

To display the Fabric Log, choose **Fabric Log** from the **Logs** menu.

- The **Date/Time** column displays the date and time of the change in the fabric.

- The **Fabric Status Changed** column displays the type of change in the fabric (for example, a switch was added or removed, an ISL was added or removed, the fabric was renamed or persisted, or a zone set became active).
- The **Description** column displays a description of the change in the fabric.

Audit Log

The switch audit log displays a history of all configuration changes made to a switch from the Product Manager simple network management protocol (SNMP) management workstation. This information is useful for system administrators and users. To open the audit log from the **Hardware View**, **Port List View**, or **Performance View**, select **Audit Log** from the **Logs** menu on the navigation control panel.

For a description of the audit log and an explanation of button functions at the bottom of the log window, refer to the switch *hp StorageWorks edge switch 2/32 product manager user guide*.

Event Log

The switch Event Log (Figure 3–3) displays a history of events for the switch, such as system events, degraded operation, FRU failures, FRU removals and replacements, port problems, Fibre Channel link incidents, and HAFM server-to-switch communication problems. All detected software and hardware failures are recorded in the Event Log. The information is useful to maintenance personnel for fault isolation and repair verification.

To open the Event Log, select **Event Log** from the **Logs** menu on the navigation control panel.

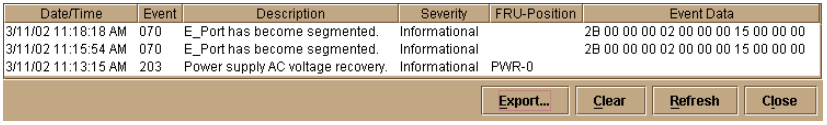

Date/Time
Event
Description
Severity
FRU-Position
Event Data
3/11/02 11:18:18 AM 070 E_Port has become segmented. Informational 2B 00 00 00 02 00 00 00 15 00 00 00
3/11/02 11:15:54 AM 070 E_Port has become segmented. Informational 2B 00 00 00 02 00 00 00 15 00 00 00
3/11/02 11:13:15 AM 203 Power supply AC voltage recovery. Informational PWR-0
Export...
Clear
Refresh
Close

Figure 3–3: Switch Event Log

The log contains the following columns:

- **Date/Time —** the date and time the switch event occurred.
- **Event —** the three-digit event code associated with the event. Refer to Appendix B for an explanation of event codes.

- **Description —** a brief description of the event.
- **Severity —** the severity of the event (Informational, Minor, Major, or Severe).
- **FRU-Position —** an acronym representing the FRU or non-FRU elements, followed by a number representing the FRU or chassis position. The acronyms are:
  - **SFP —** Small form factor pluggable (SFP) optical transceiver. Chassis slots for SFPs inserted in a port are 0 through 31. The SFPs are FRUs.
  - **PWR —** power supply. Chassis slots for redundant power supplies are 0 and 1. The power supplies are FRUs.
  - **FAN —** cooling fan. Chassis slots for redundant fans are 0 through 3. The cooling fans are FRUs.
  - **CTP —** control processor (CTP) card. The chassis slot is 0. The CTP card is not a FRU.
  - **THM —** thermal sensor. The chassis slot is 0 (on the CTP card). The thermal sensor is not a FRU.
- **Event Data —** up to 32 bytes of supplementary event data (if available for the event) in hexadecimal format. Refer to Appendix B for an explanation of the supplementary event data.

Refresh the Event Log

To ensure recently created events display in the Event Log, periodically refresh the log display. This is particularly important when inspecting the log for informational event codes to verify a repair procedure. To refresh the log, click **Refresh** at the bottom of the log window.

Clear the Event Log

To ensure the Event Log is up-to-date and not filled with archived events, periodically clear the log display. To clear the log, click **Clear** at the bottom of the log window.

Hardware Log

The Hardware Log (Figure 3–4) displays a history of FRU removals and replacements (insertions) for the switch. The information is useful to maintenance personnel for fault isolation and repair verification.

NOTE: The FRU designations in the following figure may not accurately represent the FRU designations for the Edge Switch 2/32, however they serve as examples for explanation purposes.

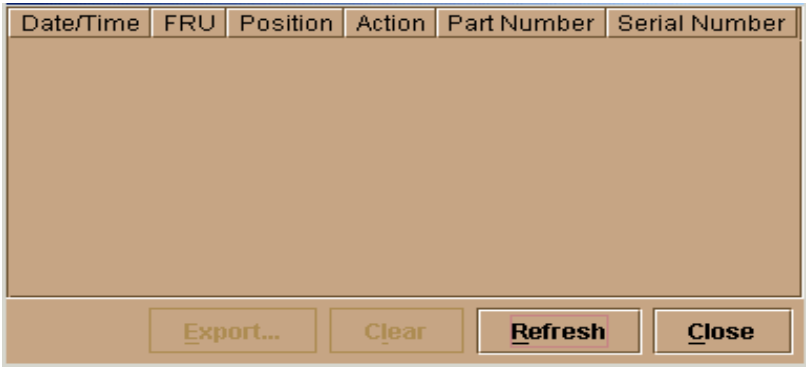


Figure 3–4: Hardware Log

To open the Hardware Log, select **Hardware Log** from the **Logs** menu on the navigation control panel.

The log contains the following columns:

- **Date/Time —** the date and time the FRU was inserted or removed.
- **FRU —** an acronym representing the FRU type or non-FRU element. The acronyms are:
  - **SFP —** Small form factor pluggable (SFP) optical transceiver. Chassis slots for SFPs inserted in a port are 0 through 31. The SFPs are FRUs.
  - **PWR —** power supply. Chassis slots for redundant power supplies are 0 and 1. The power supplies are FRUs.
  - **FAN —** cooling fan. Chassis slots for redundant fans are 0 through 3 (cooling fans). The cooling fans are FRUs.
  - **CTP —** control processor (CTP) card. The chassis slot is 0. The CTP card is not a FRU.
  - **THM —** thermal sensor. The chassis slot is 0 (on the CTP card). The thermal sensor is not a FRU.
- **Position —** a number representing the FRU chassis position. Chassis slots for power supplies are 0 and 1. Chassis slots for fans are 0 through 4 (cooling fans) inclusive. Chassis slots for SFPs are 0 through 31.
- **Action —** the action performed (Inserted or Removed).

- **Part Number —** the part number of the inserted or removed FRU.
- **Serial Number —** the serial number of the inserted or removed FRU.

Link Incident Log

The Link Incident Log (Figure 3–5) displays a history of Fibre Channel link incidents and associated port numbers for the switch. The information is useful to maintenance personnel for isolating port problems and repair verification.

To open the Link Incident Log, select **Link Incident Log** from the **Logs** menu on the navigation control panel.

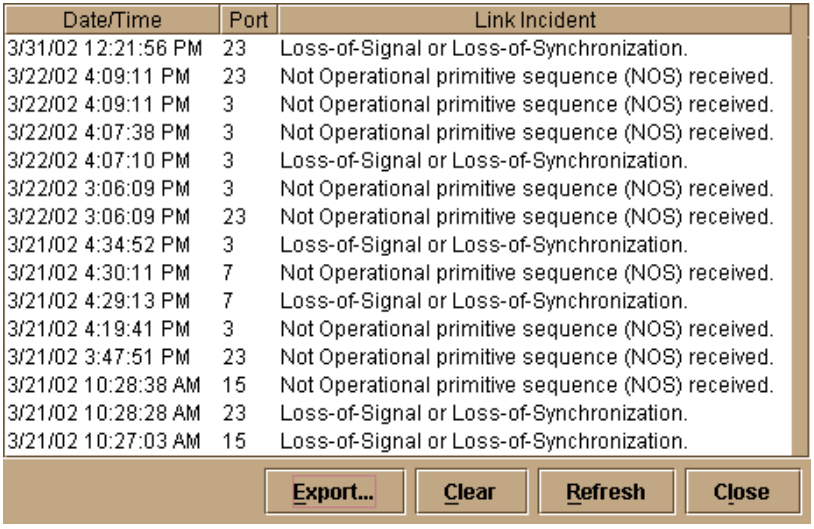

Date/Time
Port
Link Incident
3/31/02 12:21:56 PM 23 Loss-of-Signal or Loss-of-Synchronization.
3/22/02 4:09:11 PM 23 Not Operational primitive sequence (NOS) received.
3/22/02 4:09:11 PM 3 Not Operational primitive sequence (NOS) received.
3/22/02 4:07:38 PM 3 Not Operational primitive sequence (NOS) received.
3/22/02 4:07:10 PM 3 Loss-of-Signal or Loss-of-Synchronization.
3/22/02 3:06:09 PM 3 Not Operational primitive sequence (NOS) received.
3/22/02 3:06:09 PM 23 Not Operational primitive sequence (NOS) received.
3/21/02 4:34:52 PM 3 Loss-of-Signal or Loss-of-Synchronization.
3/21/02 4:30:11 PM 7 Not Operational primitive sequence (NOS) received.
3/21/02 4:29:13 PM 7 Loss-of-Signal or Loss-of-Synchronization.
3/21/02 4:19:41 PM 3 Not Operational primitive sequence (NOS) received.
3/21/02 3:47:51 PM 23 Not Operational primitive sequence (NOS) received.
3/21/02 10:28:38 AM 15 Not Operational primitive sequence (NOS) received.
3/21/02 10:28:28 AM 23 Loss-of-Signal or Loss-of-Synchronization.
3/21/02 10:27:03 AM 15 Loss-of-Signal or Loss-of-Synchronization.
Export...
Clear
Refresh
Close

Figure 3–5: Link Incident Log

The log contains the following columns:

- **Date/Time —** the date and time the link incident occurred.
- **Port —** the port number that reported the link incident (0 through 31).
- **Link Incident —** a brief description of the link incident. Problem descriptions include:
  - — Implicit incident.
  - — Bit-error threshold exceeded.
  - — Link failure **—** loss of signal or loss of synchronization.

— Link failure — not-operational primitive sequence received.

— Link failure — primitive sequence timeout.

— Link failure — invalid primitive sequence received for current link state.

Refer to "MAP 0600: Port Failure and Link Incident Analysis" on page -63 or "MAP 0700: Fabric, ISL, and Segmented Port Problem Determination" on page -79 for corrective actions in response to these link incident messages.

Refresh the Link Incident Log

To ensure recently created link incidents display in the Link Incident Log, periodically refresh the log display. To refresh the log, click **Refresh** at the bottom of the log window.

Clear the Link Incident Log

To ensure the Link Incident Log is up-to-date and not filled with archived incidents, periodically clear the log display. To clear the log, click **Clear** at the bottom of the log window.

Threshold Alert Log

This log provides details of threshold alert notifications. Besides the date and time that the alert occurred, the log also displays details about the alert as configured through the Configure Threshold Alert(s) option under the **Configure** menu.

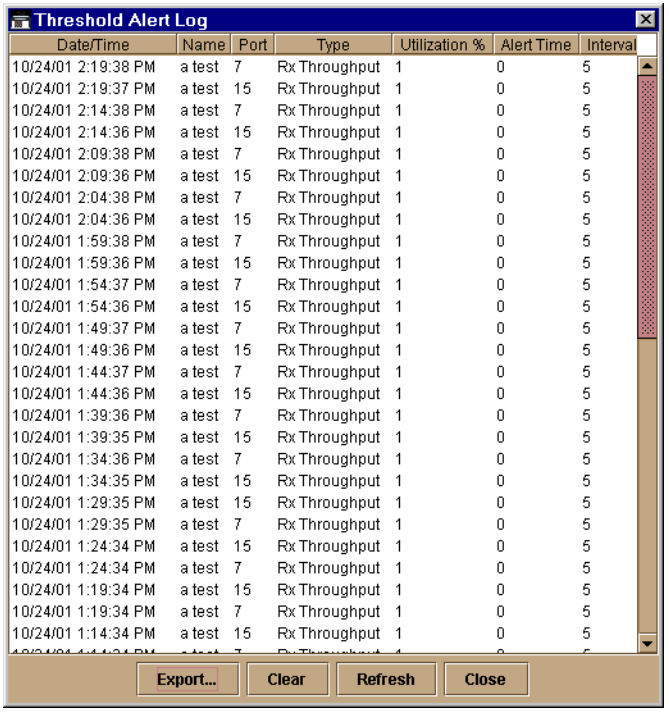

Threshold Alert Log
Date/Time Name Port Type Utilization % Alert Time Interval
10/24/01 2:19:38 PM a test 7 Rx Throughput 1 0 5
10/24/01 2:19:37 PM a test 15 Rx Throughput 1 0 5
10/24/01 2:14:38 PM a test 7 Rx Throughput 1 0 5
10/24/01 2:14:36 PM a test 15 Rx Throughput 1 0 5
10/24/01 2:09:38 PM a test 7 Rx Throughput 1 0 5
10/24/01 2:09:36 PM a test 15 Rx Throughput 1 0 5
10/24/01 2:04:38 PM a test 7 Rx Throughput 1 0 5
10/24/01 2:04:36 PM a test 15 Rx Throughput 1 0 5
10/24/01 1:59:38 PM a test 7 Rx Throughput 1 0 5
10/24/01 1:59:36 PM a test 15 Rx Throughput 1 0 5
10/24/01 1:54:37 PM a test 7 Rx Throughput 1 0 5
10/24/01 1:54:36 PM a test 15 Rx Throughput 1 0 5
10/24/01 1:49:37 PM a test 7 Rx Throughput 1 0 5
10/24/01 1:49:36 PM a test 15 Rx Throughput 1 0 5
10/24/01 1:44:37 PM a test 7 Rx Throughput 1 0 5
10/24/01 1:44:36 PM a test 15 Rx Throughput 1 0 5
10/24/01 1:39:36 PM a test 7 Rx Throughput 1 0 5
10/24/01 1:39:35 PM a test 15 Rx Throughput 1 0 5
10/24/01 1:34:36 PM a test 7 Rx Throughput 1 0 5
10/24/01 1:34:35 PM a test 15 Rx Throughput 1 0 5
10/24/01 1:29:35 PM a test 15 Rx Throughput 1 0 5
10/24/01 1:29:35 PM a test 7 Rx Throughput 1 0 5
10/24/01 1:24:34 PM a test 15 Rx Throughput 1 0 5
10/24/01 1:24:34 PM a test 7 Rx Throughput 1 0 5
10/24/01 1:19:34 PM a test 15 Rx Throughput 1 0 5
10/24/01 1:19:34 PM a test 7 Rx Throughput 1 0 5
10/24/01 1:14:34 PM a test 15 Rx Throughput 1 0 5
Export...
Clear
Refresh
Close

Figure 3–6: Threshold Alert Log

- **Date/Time**

  Date and time stamp for when the alert occurred.

- **Name**

  Name for the alert as configured through the **Configure Threshold Alerts** dialog box.

- **Port**

  Port number where the alert occurred.

- **Type**

  The type of alert: transmit (TX) or receive (RX).

- **Utilization %**

Percent usage of traffic capacity. This is the percent of the port's throughput capacity achieved by the measured throughput. This setting constitutes the threshold value and is configured through the **Configure Threshold Alerts** dialog box. For example, a value of 25 means that threshold occurs when throughput reaches 25 percent of the port's capacity.

- **Alert Time**

  The time that the utilization % must exist before an alert is generated. This is set through the **Configure Threshold Alerts** dialog box.

- **Interval**

  The time interval during which the throughput is measured and an alert can generate. This is set through the **Configure Threshold Alerts** dialog box.

Using Views

The HAFM and Product Manager provide access to a series of views (windows) that provide information for administrators, users, and maintenance personnel. These views are accessed through the **Hardware View**, and include the:

- **Port List View**.
- **FRU List View**.
- **Node List View**.
- **Performance View**.
- **Topology View**.
- **Zoning View**.

Port List View

The **Port List View** (Figure 3–7) lists and provides status information for all switch ports. The information is useful to maintenance personnel for isolating port problems.

To open the **Port List View**, select **Port List** from the **View** menu on the navigation control panel.

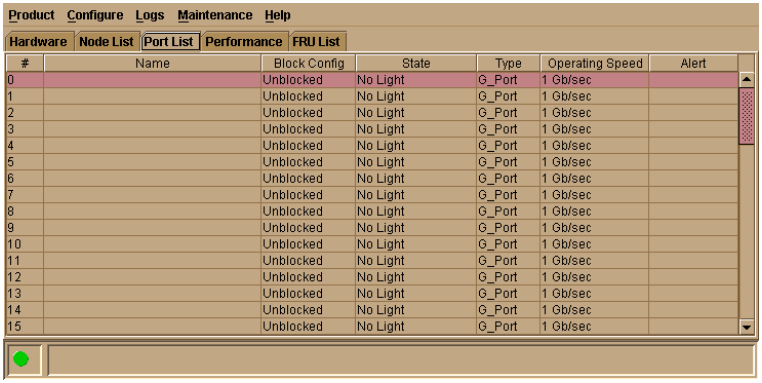

Product Configure Logs Maintenance Help
Hardware Node List Port List Performance FRU List
Name Block Config State Type Operating Speed Alert
0 Unblocked No Light G_Port 1 Gb/sec
1 Unblocked No Light G_Port 1 Gb/sec
2 Unblocked No Light G_Port 1 Gb/sec
3 Unblocked No Light G_Port 1 Gb/sec
4 Unblocked No Light G_Port 1 Gb/sec
5 Unblocked No Light G_Port 1 Gb/sec
6 Unblocked No Light G_Port 1 Gb/sec
7 Unblocked No Light G_Port 1 Gb/sec
8 Unblocked No Light G_Port 1 Gb/sec
9 Unblocked No Light G_Port 1 Gb/sec
10 Unblocked No Light G_Port 1 Gb/sec
11 Unblocked No Light G_Port 1 Gb/sec
12 Unblocked No Light G_Port 1 Gb/sec
13 Unblocked No Light G_Port 1 Gb/sec
14 Unblocked No Light G_Port 1 Gb/sec
15 Unblocked No Light G_Port 1 Gb/sec

Figure 3–7: Port List View

The port row provides status information in the following columns:

- **Port # —** the port number (0 through 31).
- **Addr —** the switch logical port address in hexadecimal format (S/390 operating mode only).
- **Name —** the port name configured through the **Configure Ports** dialog box.
- **Blocked Config —** the status (Blocked or Unblocked) of the port.
- **State —** the state of the port. Valid states are:
  - — Online, offline, or testing.
  - — Beaconing.
  - — Invalid Attachment.
  - — Link incident or link reset
  - — No light, not operational, or port failure.
  - — Segmented E_Port.
- **Type —** The type of port. Valid port types are a generic port (G_Port) that is not connected to a Fibre Channel device or switch, therefore light is not transmitted; fabric port (F_Port) that is connected to a device; or an expansion port (E_Port) that is connected to another switch to form an interswitch link (ISL).
- **Operating Speed —** The speed at which the port is operating

- **Alert —** If link incident (LIN) alerts are configured for the port through the **Configure Ports** dialog box, a yellow triangle displays in the column when a link incident occurs. A yellow triangle also displays if beaconing is enabled for the port. A red and yellow diamond displays if the port fails.

Click anywhere in the port row to open the **Port Properties** dialog box. Right-click anywhere in the port row to open a menu to:

- Open the **Port Properties** dialog box.
- Open the **Node Properties** dialog box.
- Display the **Port Technology** dialog box.
- Block or unblock the port.
- Enable port beaconing.
- Perform port diagnostics.
- Enable or disable port channel wrapping. This menu option displays only when the switch is configured for S/390 operating mode.
- Swap one Fibre Channel port address with another. This menu option displays only when the switch is configured for S/390 operating mode.
- Clear link incident alerts.
- Reset the port.
- Configure Port Binding.

FRU List View

The **FRU List View** (Figure 3–8 on page 3-15) displays a list of all switch FRUs. The information is useful to maintenance personnel for fault isolation and repair verification.

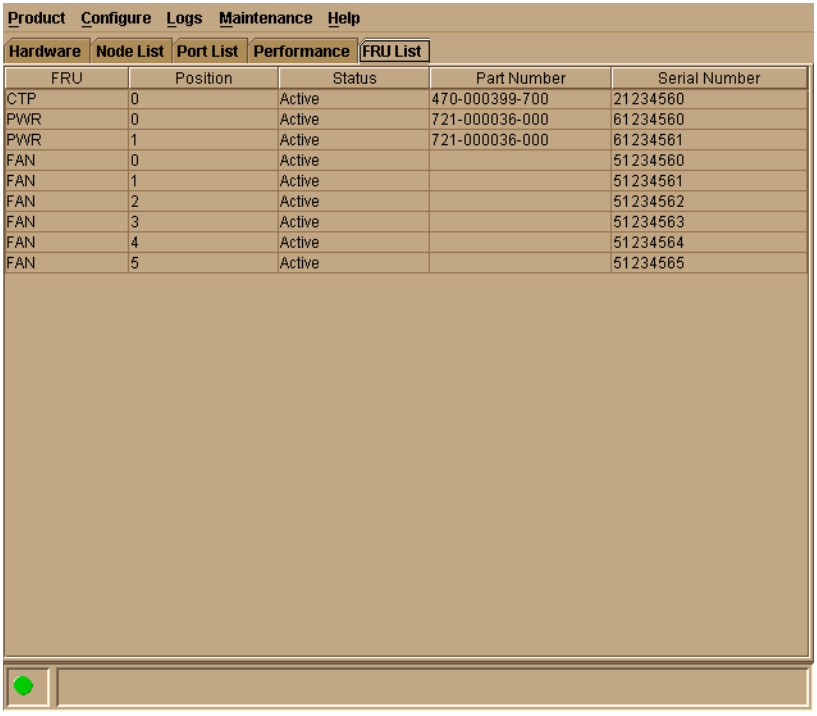

Product Configure Logs Maintenance Help
Hardware Node List Port List Performance FRU List
FRU Position Status Part Number Serial Number
CTP 0 Active 470-000399-700 21234560
PWR 0 Active 721-000036-000 61234560
PWR 1 Active 721-000036-000 61234561
FAN 0 Active 51234560
FAN 1 Active 51234561
FAN 2 Active 51234562
FAN 3 Active 51234563
FAN 4 Active 51234564
FAN 5 Active 51234565

Figure 3–8: FRU List View

To open the **FRU List View** from the **Hardware View**, click **View** and select **FRU List**. The **FRU List View** contains the following columns:

- **FRU —** an acronym representing the FRU type. FRU acronyms are:
  - **SFP —** Small form factor pluggable (SFP) optical transceiver. Chassis slots for SFPs inserted in a port are 0 through 31. The SFPs are FRUs.
  - **PWR —** power supply. Chassis slots for redundant power supplies are 0 and 1. The power supplies are FRUs.
  - **FAN —** cooling fan. Chassis slots for redundant fans are 0 through 4 (cooling fans). The cooling fans are FRUs.
  - **CTP —** control processor (CTP) card. The chassis slot is 0. The CTP card is not a FRU.

— **THM —** thermal sensor. The chassis slot is 0 (on the CTP card). The thermal sensor is not a FRU.

- **Position**-a number representing the FRU chassis position. The chassis (slot) position for a nonredundant FRU is 0. The chassis positions for redundant FRUs are 0 and 1.
- **Status-**the FRU status (Active or Backup).
- **Part Number**-the FRU part number.
- **Serial Number**-the FRU serial number.

Node List View

The **Node List View** (Figure 3–9) displays information about all devices attached to the switch through node ports (N_Ports). The information is useful to maintenance personnel for fault isolation and repair verification.

To open the **Node List View**, select **Node List** from the **View** menu on the navigation control panel.

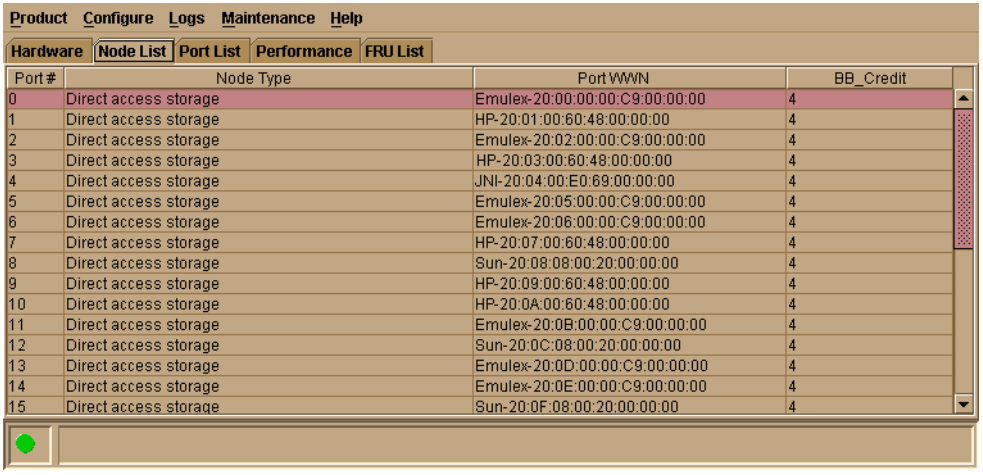

Product Configure Logs Maintenance Help
Hardware Node List Port List Performance FRU List
Port # Node Type Port WWN BB_Credit
0 Direct access storage Emulex-20:00:00:00:C9:00:00:00 4
1 Direct access storage HP-20:01:00:60:48:00:00:00 4
2 Direct access storage Emulex-20:02:00:00:C9:00:00:00 4
3 Direct access storage HP-20:03:00:60:48:00:00:00 4
4 Direct access storage JNI-20:04:00:E0:69:00:00:00 4
5 Direct access storage Emulex-20:05:00:00:C9:00:00:00 4
6 Direct access storage Emulex-20:06:00:00:C9:00:00:00 4
7 Direct access storage HP-20:07:00:60:48:00:00:00 4
8 Direct access storage Sun-20:08:08:00:20:00:00:00 4
9 Direct access storage HP-20:09:00:60:48:00:00:00 4
10 Direct access storage HP-20:0A:00:60:48:00:00:00 4
11 Direct access storage Emulex-20:0B:00:00:C9:00:00:00 4
12 Direct access storage Sun-20:0C:08:00:20:00:00:00 4
13 Direct access storage Emulex-20:0D:00:00:C9:00:00:00 4
14 Direct access storage Emulex-20:0E:00:00:C9:00:00:00 4
15 Direct access storage Sun-20:0F:08:00:20:00:00:00 4

Figure 3–9: Node List View

The **Node List View** contains the following columns:

- **Port # —** the port number (0 through 31). Only ports attached to a device are displayed.

- **Addr —** the switch logical port address (05 through 23 inclusive) in hexadecimal format (S/390 operating mode only).
- **Node Type —** the type of attached device. This information is supplied by the device (if supported). Node types include:
  - — Unknown or other.
  - — Hub, switch, gateway, or converter.
  - — Host or host bus adapter (HBA).
  - — Proxy agent.
  - — Storage device or storage subsystem.
  - — Module.
  - — Software driver.
- **Port WWN-** the eight-byte (16-digit) worldwide name (WWN) assigned to the port or Fibre Channel interface installed on the attached device.
  - — If a nickname is not assigned to the WWN, the WWN is prefixed by the device manufacturer's name.
  - — If a nickname is assigned to the WWN, the nickname displays in place of the WWN.
- **BB_Credit —** the buffer-to-buffer credit (BB_Credit) value assigned to a port attached to a device. The value (normally 1 through 16 inclusive) determines the frame buffers available for the port. Ports configured for extended distance operation are assigned a BB_Credit value of 60.

Performance View

The **Performance View** displays statistical information about the performance of the ports. The information is useful to maintenance personnel for isolating port problems. For information about the **Performance View**, refer to "Performing Port Diagnostics" on page -19.

Zone Set View

The **Zone Set View** (Figure 3–10) displays a list of the active zone set, including all zones and zone members. The active zone set name displays at the top of the list, followed by zone names, followed by zone members for each name.The table at the top of the view indicates if the default zone is enabled or disabled.

To open the **Zone Set View**, click the **Zone Set** tab at the bottom of the **Fabrics View** on the HAFM main window.

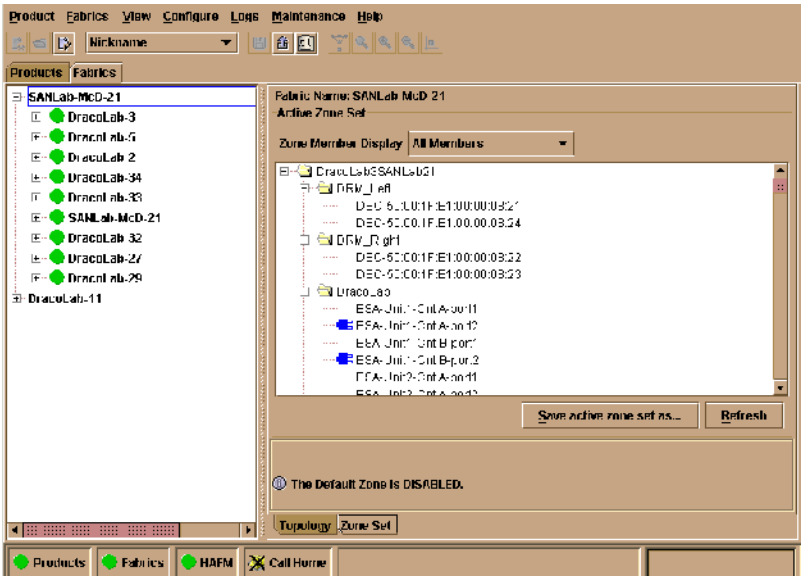


Figure 3–10: Zone Sets View

Zone members are displayed as:

- The unique 16-digit WWN identifying the device attached to the port. If a nickname is configured, the nickname displays instead. For example:

  10:00:0206:77:43:B0:1C

- A unique domain ID (1 through 31 inclusive) and port number (0 through 31). For example:

  Domain 1, Port 7

The information is also useful for fault isolating E_Port segmentation problems caused by incompatible zone sets. When forming a multi-switch fabric by connecting switches with active zone sets, zone names within the active zone sets should not be duplicated. Names can be duplicated only if the member WWNs of each zone are

identical. If two switches have a zone name conflict (duplicate zone names exist), the zone sets cannot merge, the connecting E_Port at each switch segments to prevent the creation of an ISL, and the switches do not form a multi-switch fabric.

For a description of how to expand or collapse the active zone set list and an explanation of button functions at the bottom of the **Zoning View**, refer to the *hp StorageWorks High Availability Fabric Manager user guide*.

Performing Port Diagnostics

Port diagnostics are performed at the switch and *Product Manager* application. These diagnostics include:

- Inspecting port light-emitting diodes (LEDs) at the switch.
- Obtaining port degradation or failure information at the *Product Manager* application's **Hardware View**.
- Obtaining statistical performance information for ports at the *Product Manager* application's **Performance View.**
- Performing internal or external port loopback tests.
- Performing channel wrap tests. The tests apply only to a switch configured for S/390 operating mode.

Port LEDs

To obtain port operational information at the switch, inspect the port LEDs. Amber and green LEDs adjacent to each port indicate operational status as follows:

- The green LED illuminates (or blinks if there is active traffic) and the amber LED extinguishes to indicate normal port operation.
- The amber LED illuminates and the green LED extinguishes to indicate a port failure.
- Both LEDs extinguish to indicate a port is operational but not communicating (no SFP installed, no cable attached, loss of light, port blocked, or link recovery in process).
- The amber LED flashes and the green LED illuminates (or blinks if there is active traffic) to indicate beaconing is set for the port.

- The amber LED flashes and the green LED extinguishes to indicate a port is running online diagnostics, or beaconing is set and the port is not communicating (no SFP installed, no cable attached, loss of light, port blocked, or link recovery in process).

Hardware View

The **Hardware View** (Figure 3–11) displays a representation of and associated information about a specified switch. This information is useful to maintenance personnel for port-specific fault isolation and repair verification, link incidents, and port segmentation problems.

- Port operational state information from the **Port Properties** dialog box (Figure 3–12).
- Port LED behavior that emulates the operational status of the corresponding real switch. Refer to Table 1–1 on page 1-23 for an explanation of green and amber LED behavior.
- Colored alert symbols (yellow triangle or red diamond with yellow background) that indicate port status. Refer to Table 1–1 on page 1-23 for an explanation of alert symbol indications.

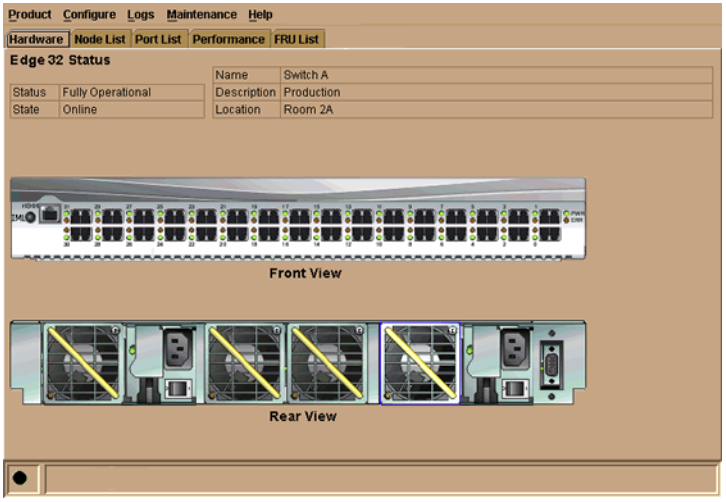


Figure 3–11: Hardware View

Click the port connector (leftmost port) to open the **Port Properties** dialog box (Figure 3–12).

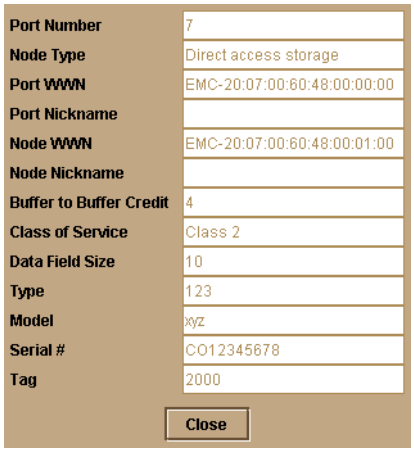


Figure 3–12: Port Properties Dialog Box

The dialog box provides the following information:

- **Port Number —** the switch port number (0 through 31).
- **Port Name —** the user-defined name or description for the port.
- **Type —** the type of port (G_Port if nothing is attached to the port, F_Port if a device is attached to the port, and E_Port if the port is connected to another switch as part of an ISL).
- **Fibre Channel Address —** the Fibre Channel address identifier for the port.
- **Port WWN —** the Fibre Channel WWN for the port.
  - — If a nickname is not assigned to the WWN, the WWN is prefixed by the device manufacturer's name.
  - — If a nickname is assigned to the WWN, the nickname displays in place of the WWN.
- **Attached Port WWN —** the Fibre Channel WWN for the device attached to the port.
- **Block Configuration —** a user-configured state for the port (Blocked or Unblocked).
- **10-100 km Configuration —** a user-specified state for the port (On or Off), configured through the **Configure Ports** dialog box.

- **LIN Alerts Configuration —** a user-specified state for the port (On or Off), configured through the **Configure Ports** dialog box.
- **Beaconing —** user-specified for the port (On or Off). When beaconing is enabled, a yellow triangle displays adjacent to the **Status** field.
- **Link Incident —** If no link incidents are recorded, None displays in the **Status** field. If a link incident is recorded, a summary displays describing the incident, and a yellow triangle displays adjacent to the **Status** field. Valid summaries are:
  - Implicit incident.
  - Bit-error threshold exceeded.
  - Link failure **—** loss of signal or loss of synchronization.
  - Link failure **—** not-operational primitive sequence received.
  - Link failure **—** primitive sequence timeout.
  - Link failure **—** invalid primitive sequence received for the current link state.
- **Operational State —** the state of the port (Online, Offline, Beaconing, Invalid Attachment, Link Incident, Link Reset, No Light, Not Operational, Port Failure, Segmented E_Port, or Testing). A yellow triangle displays adjacent to the **Status** field if the port is in a non-standard state that requires attention. A red and yellow diamond displays adjacent to the **Status** field if the port fails.
- **Reason —** If the E_Port segments while attempting to form a multi-switch fabric, a summary displays describing the reason for segmentation. Valid summaries are:
  - Incompatible operating parameters.
  - Duplicate domain ID(s).
  - Incompatible zoning configurations.
  - Build fabric protocol error.
  - No principal switch.
  - No response from attached switch.
  - Exchange link protocol (ELP) retransmission failure timeout.

This field also displays reasons for Invalid Attachment state:

- 01 Unknown. Invalid attachment reason cannot be determined.
- 02 ISL connection not allowed on this port. Port is configured as an F_Port, but connected to switch or director.

- 03 ELP rejected by the attached switch. This director/switch transmitted an exchange link protocol (ELP) frame that was rejected by the switch at the other end of the ISL.
- 04 Incompatible switch at the other end of the ISL. Interop mode for this switch is set to Open Fabric mode and the switch at the other end of the ISL is an HP switch configured for Homogeneous Fabric mode.
- 05 External loopback adapter connected to the port. A loopback plug is connected to the port and there is no diagnostic test running.
- 06 N_Port connection not allowed on this port. The port type configuration does not match the actual port use. Port is configured as an E_Port, but attaches to a node device.
- 07 Non-HP switch at other end of the ISL. The cable is connected to a non-HP switch and interop mode is set to Homogeneous fabric mode.
- 08 ISL connection not allowed on this port. The port type configuration does not match the actual port use (the port is configured as an F_Port, but attaches to a switch or director).
- 10 Port binding violation **—** unauthorized WWN. The WWN entered to configure port binding is not valid or a nickname was used that is not configured through the Product Manager for the attached device.
- 11 Unresponsive node connected to port. Possible causes are:
  - — Hardware problem on switch or on a connected node where ELP frames are not delivered, the response is not received, or a fabric login in (FLOGI) cannot be received. There may be problems in switch SBAR.
  - — Faulty or dirty cable connection.
  - — Faulty host bus adapters that do not send out FLOGI within reasonable time frame.
- **Threshold Alert —** If a threshold alert exists for the port, an alert indicator (yellow triangle) will display by the **Threshold Alert** field, and the configured name for the last alert received will display in the field.

Performance View

The **Performance View** (Figure 3–13) displays statistical information about the performance of the ports. The information is useful for isolating port problems. To open the **Performance View** from the **Hardware View**, select **Performance** from the **View** menu on the navigation control panel.

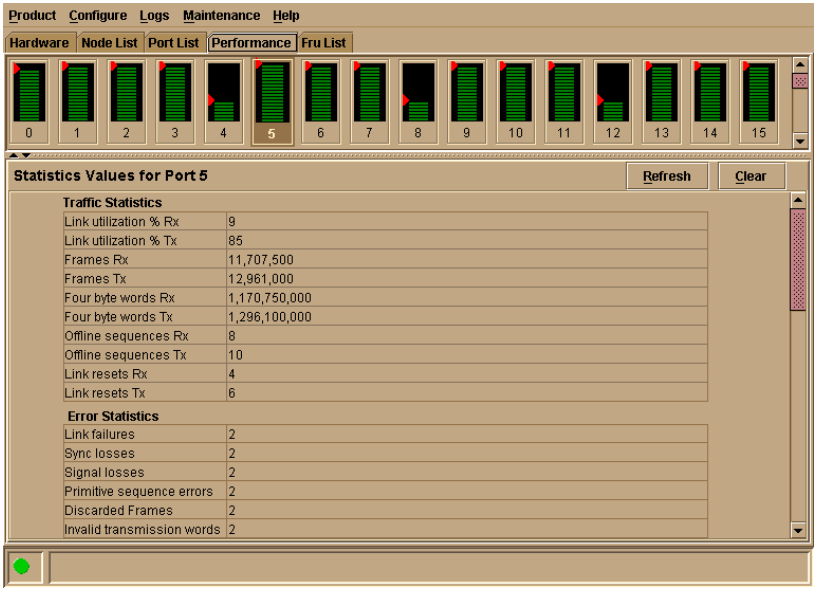

Product Configure Logs Maintenance Help
Hardware Node List Port List Performance Fru List
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
Statistics Values for Port 5
Refresh
Clear
Traffic Statistics
Link utilization % Rx 9
Link utilization % Tx 85
Frames Rx 11,707,500
Frames Tx 12,961,000
Four byte words Rx 1,170,750,000
Four byte words Tx 1,296,100,000
Offline sequences Rx 8
Offline sequences Tx 10
Link resets Rx 4
Link resets Tx 6
Error Statistics
Link failures 2
Sync losses 2
Signal losses 2
Primitive sequence errors 2
Discarded Frames 2
Invalid transmission words 2

Figure 3–13: Performance View

When the **Performance View** opens, no port statistics or errors display. The message `Click on gauge above to display statistics for that port` displays beneath the port bar graphs.

Each port bar graph in the upper portion of the view displays the instantaneous transmit or receive activity level for the port, and is updated every five seconds. The relative value displayed is the greater of either the transmit or receive activity (whichever value is greatest when sampled). Each port's graph has multiple green-bar level indicators that correspond to a percentage of the maximum Fibre Channel throughput for the port (either transmit or receive). If any activity is detected for a port, at least one green bar displays.

A red indicator on each port bar graph (high-water mark) remains at the highest level the graph has reached since the **Performance View** was opened. The indicator does not display if the port is offline, and is reset to the bottom of the graph if the port detects a loss of light.

When the mouse pointer is passed over a port bar graph, the graph highlights with a blue border and an information pop-up displays adjacent to the port as follows:

- If a device is not attached to the port, the pop-up displays the port's current state.

- If a device is attached to the port, the pop-up displays the WWN of the attached device.
- If the port is an E_Port, the pop-up displays E_Port.
- If the port is segmented, the pop-up displays Segmented E_Port.

Click a port bar graph to display statistics values for the port (bottom half of the **Performance View**). Right-click a port bar graph to display statistics values for the port (bottom half of the **Performance View**) and access a menu to:

- Open the **Port Properties**, **Node Properties**, or **Port Technology** dialog boxes.
- Block or unblock the port.
- Enable or disable port beaconing.
- Perform port diagnostics.
- Enable or disable port channel wrapping. This menu option displays only when the switch is configured for S/390 operating mode.
- Swap one Fibre Channel port address with another. This menu option displays only when the switch is configured for S/390 operating mode.
- Clear link incident alerts.
- Reset the port.
- Configure Port Binding.

When a port is selected, the bottom half of the **Performance View** displays the following tables of cumulative port statistics and error count values. These statistics correspond to values defined in the Fabric Element management information base (MIB).

- Traffic statistics.
- Class 2 statistics.
- Class 3 statistics.
- Error statistics.

Click the **Refresh** button to update statistical information displayed on the **Performance View** for the selected port. Click the **Clear** button to reset the cumulative value counts to zero on the **Performance View** for the selected port. A confirmation dialog box displays before the values are cleared.

Perform Loopback Tests

This section describes procedures to perform an:

- **Internal loopback test —** an internal loopback test checks internal port, serializer, and deserializer circuitry and checks for the presence of a SFP, but does not check fiber-optic components of the installed SFP. The test can be performed with a switch or device attached to a port.The test momentarily blocks the port and is disruptive to the attached device.
- **External loopback test —** an external loopback test checks all port circuitry, including fiber-optic components of the installed SFP. To perform the test, the attached switch or device must be quiescent and disconnected from the port, and a multi-mode or single-mode loopback plug must be inserted in the SFP receptacle.

Internal Loopback Test

To perform an internal loopback test for a single port:

1. Notify the customer that a disruptive internal loopback test is to be performed on a port. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port and sets the attached devices offline.

NOTE: An SFP transceiver must be installed in the port during the test. A switch can remain attached during the test.

2. At the HAFM server, open the *HAFM* application. The **Product View** displays.
3. Select the icon representing the switch to be tested. The **Hardware View** for the selected switch displays.
4. At the **Hardware View**, verify the location of the port to be tested. When the mouse pointer is passed over the graphical port on the front view of the switch, the port highlights with a blue border and an pop-up displays Switch Port.
5. At the navigation control panel, select **Port Diagnostics** from the **Maintenance** menu. The **Port Diagnostics** dialog box displays (Figure 3–14).
6. Select a port for test. To select a port for test, type the port number (0 through 31) in the **Port Number** field.
7. At the **Diagnostics Test** list box, select **Internal Loopback**.

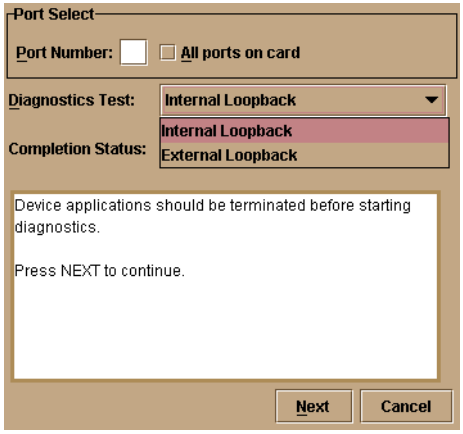


Figure 3–14: Port Diagnostics Dialog Box

8. Click **Next**. Beaconing initiates for the port selected for test. At the **Hardware View**, a yellow triangle displays at the top of the port. At the **Port Diagnostics** dialog box, the message `Verify selected ports are beaconing` displays.
9. Verify beaconing is enabled, then click **Next**. The message `Press START Test to begin diagnostics` displays, and the **Next** button changes to a **Start Test** button.
10. Click **Start Test**. The test begins and:
    - — The **Start Test** button changes to a **Stop Test** button
    - — The message `Port xx: Test running` displays, where *xx* is the port number.
    - — A red progress bar (indicating percent completion) travels from left to right across the **Completion Status** field.

    As a port is tested, the amber LED flashes (beacons) and the green LED extinguishes (indicating the port is blocked).

NOTE: Click **Stop Test** at any time to abort the loopback test.

11. When the test completes, test results display (for each port tested) as `Port xx: Test Passed!` or `Port xx: Failed!` in the message area of the dialog box. If a port fails the test, the amber LED for the port remains illuminated.

12. When finished, click **Cancel** to close the **Port Diagnostics** dialog box and return to the **Hardware View**. Beaconing is disabled for the port.
13. Reset each tested port.

External Loopback Test

To perform an external loopback test for a single port:

1. Notify the customer that a disruptive external loopback test will be performed on a port and the fiber-optic cable or cables will be disconnected. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port and sets attached devices offline.

NOTE: At the start of the loopback test, the port can be online, offline, blocked, or unblocked.

2. At the HAFM server, open the *HAFM* application. The **Product View** displays.
3. Select the icon representing the switch for which the loopback test is to be performed. The **Hardware View** for the selected switch displays.
4. At the **Hardware View**, verify the location of the port to be tested. When the mouse pointer is passed over the graphical port on the front view of the switch, the port highlights with a blue border and an pop-up displays Switch Port.
5. Disconnect the fiber-optic jumper cable from the port.

CAUTION: If name server zoning is implemented for the switch by port number, ensure the fiber-optic cables that are disconnected to perform the loopback test are reconnected properly. A change to the cable configuration disrupts zone operation and may incorrectly include or exclude a device from a zone.

6. If the port to be tested is shortwave laser (determined in step 4), insert a black multi-mode loopback plug into the port receptacle. If the port to be tested is longwave laser (also determined in step 4), insert a blue single-mode loopback plug into the port receptacle.
7. At the navigation control panel, select **Port Diagnostics** from the **Maintenance** menu. The **Port Diagnostics** dialog box displays (Figure 3–14).
8. Select a port for test. To select a port for test, type the port number (0 through 31) in the **Port Number** field.
9. At the **Diagnostics Test** list box, select **External Loopback**.

10. Click **Next**. Beaconing initiates for the port selected for test. At the **Hardware View**, a yellow triangle displays at the top of the port. At the **Port Diagnostics** dialog box, the message `Loopback plug(s) must be installed on ports being diagnosed` displays.
11. Verify loopback plug(s) are installed and click **Next**. The message `Verify selected ports are beaconing` displays.
12. Verify beaconing is enabled, then click **Next**. The message `Press START TEST to begin diagnostics` displays, and the **Next** button changes to a **Start Test** button.
13. Click **Start Test**. The test begins and:
    - The **Start Test** button changes to a **Stop Test** button
    - The message `Port xx: TEST RUNNING` displays, where *xx* is the port number.
    - A red progress bar (indicating percent completion) travels from left to right across the **Completion Status** field.

    As a port is tested, the amber LED flashes (beacons) and the green LED illuminates (indicating loopback traffic through the port).

NOTE: Click **Stop Test** at any time to abort the loopback test.

14. When the test completes, test results display (for each port tested) as `Port xx: Test Passed!` or `Port xx: Failed!` in the message area of the dialog box. If a port fails the test, the amber LED for the port remains illuminated.
15. When finished, click **Cancel** to close the **Port Diagnostics** dialog box and return to the **Hardware View**. Beaconing is disabled for the port.
16. Reset each tested port.
17. Remove loopback plug(s) from the tested ports.
18. Reconnect fiber-optic jumper cables from devices to tested ports.

Perform Channel Wrap Test

A channel wrap test is a diagnostic procedure that checks S/390 host-to-switch connectivity by returning the output of the host as input. The test is host-initiated, and transmits Fibre Channel frames to a switch port. A port enabled for channel wrapping echoes the frame back to the host.

To perform a channel wrap test for a single port (S/390 mode only):

1. Notify the customer that a disruptive channel wrap test will be performed on a host-attached port.
2. At the HAFM server, open the *HAFM* application. The **Product View** displays.
3. Select (click) the icon representing the switch for which the channel wrap test will be performed. The **Hardware View** for the selected switch displays.
4. At the **Hardware View**, verify the location of the port to be tested. Click the port to be tested. The **Port View** displays.
5. Right-click the port to be tested, then select **Channel Wrap** from the pop-up menu. The **Channel Wrap On for Port *n*** (where *n* is the port number) dialog box displays (Figure 3–15).

Figure 3–15: Channel Wrap On for Port *n* Dialog Box

6. Click **OK** to enable channel wrapping for the port.

Swapping Ports

Use the port swap procedure to swap a device connection and logical port address from a failed Fibre Channel port to an operational port. Because both ports are blocked during the procedure, switch communication with the attached device is momentarily disrupted.

To perform the port swap procedure for a pair of switch ports (S/390 mode only):

1. Notify the customer a port swap procedure will be performed and a fiber-optic cable or cables will be disconnected. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the ports and sets attached devices offline.
2. At the HAFM server, open the *HAFM* application. The **Product View** displays.
3. Select (click) the icon representing the switch for which the loopback test will be performed. The **Hardware View** for the selected switch displays.

4. At the navigation control panel, select **Swap Ports** from the **Maintenance** menu. The **Swap Ports** dialog box displays (Figure 3–16).

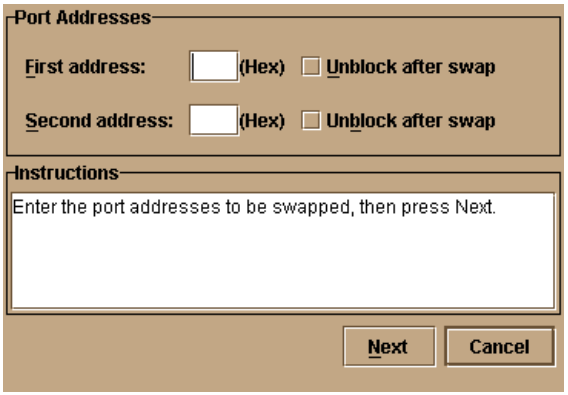


Figure 3–16: Swap Ports Dialog Box

5. At the **First address** and **Second address** fields, type the logical port addresses (in hexadecimal format) of the pair of ports to be swapped. The ports are automatically blocked during the procedure. Select the **Unblock after swap** check boxes to unblock the ports when the procedure completes.
6. Click **Next**. At the **Swap Ports** dialog box, the message `Continuing this procedure requires varying the selected ports offline. Ask the system operator to vary the link(s) offline, then press Next.` displays.
7. Click **Next**. At the **Swap Ports** dialog box, the message `Move the port cable(s). Then press Next.` displays.
8. Swap the fiber-optic jumper cables between the selected ports, then click **Next**.
9. At the **Swap Ports** dialog box, the message `Ports swapped successfully.` displays. Click **Next** to close the dialog box and return to the **Hardware View**.

Collecting Maintenance Data

When the switch operational firmware detects a critical error, the switch automatically copies the contents of dynamic random access memory (DRAM) to a dump area in FLASH memory on the CTP card, then transfers (through the Ethernet connection) the captured dump file from FLASH memory to the HAFM server hard drive.

Perform the maintenance data collection procedure after a firmware fault is corrected or a failed FRU is replaced to capture the data for analysis by third-level support personnel. Maintenance data includes the dump file, hardware log, audit log, and an engineering log viewable only by support personnel. To collect maintenance data:

1. At the HAFM server, open the *HAFM* application. The **Product View** displays.
2. Select the icon representing the switch for which the data collection procedure is to be performed. The **Hardware View** for the selected switch displays.
3. At the navigation control panel, select **Data Collection** from the **Maintenance** icon. The **Save Data Collection** dialog box (Figure 3–17) displays.

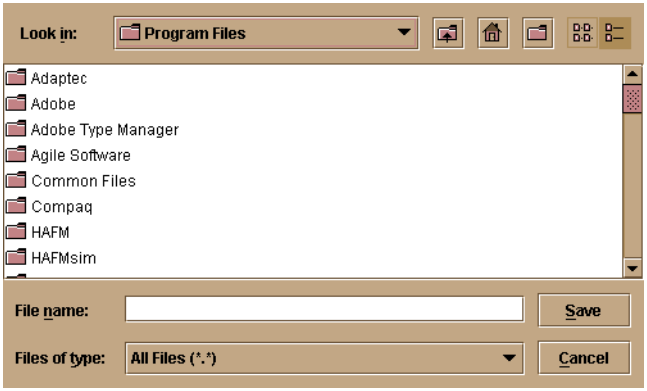


Figure 3–17: Save Data Collection Dialog Box

4. Remove the backup disk from the HAFM server Zip drive and insert a blank Zip disk.
5. At the **Save Data Collection** dialog box, select the zip drive (D:\) from the Look in drop-down menu, then type a descriptive name for the collected maintenance data in the **File name** field. Click **Save**.

6. A dialog box (Figure 3–18) displays with a progress bar that shows percent completion of the data collection process. When the process reaches 100%, the **Cancel** button changes to a **Close** button.

Figure 3–18: Data Collection Dialog Box

7. Click **Close** to close the dialog box.
8. Remove the Zip disk with the newly collected maintenance data from the HAFM server Zip drive. Return the Zip disk to HP for failure analysis.
9. To ensure the *QuikSync* backup application operates normally, replace the original backup disk in the HAFM server Zip drive.

Clean Fiber-Optic Components

Perform this procedure as directed in this publication and when connecting or disconnecting fiber-optic cables from switch SFP optical transceivers (if necessary). To clean fiber-optic components:

1. Obtain the appropriate tools (a can of oil-free, compressed air (filtered to .01 micron), CLETOP 1.25mm cleaning sticks, and isopropyl alcohol) from the fiber-optic cleaning kit.
2. Disconnect the fiber-optic cable from the SFP. Use compressed air to blow any contaminants from the connector as shown in part A of Figure 3–19.
   - — Keep the air nozzle approximately 50 millimeters (two inches) from the end of the connector and hold the can upright.
   - — Blow compressed air on the surfaces and end of the connector continuously for approximately five seconds.

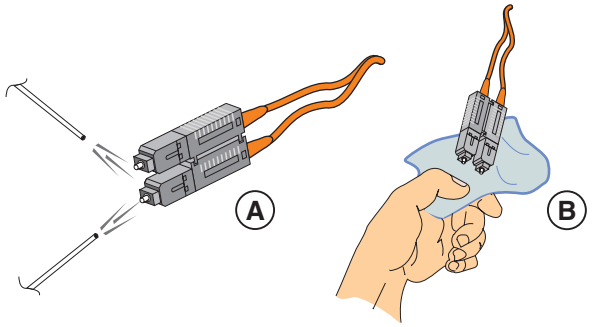


Figure 3–19: Clean Fiber-Optic Components

3. Gently wipe the end-face and other surfaces of the connector with an alcohol pad as shown in part B of Figure 3–19. Ensure the pad makes full contact with the surface to be cleaned. Wait approximately five seconds for surfaces to dry.
4. Repeat step 2 and step 3 of this procedure (second cleaning).
5. Repeat step 2 and step 3 of this procedure again (third cleaning), then reconnect the fiber-optic cable to the port.

Power-On Procedure

To power-on the switch:

1. One alternating current (AC) power cord is required for each power supply. Ensure power cord(s) are available to connect the switch to facility power.

WARNING: An HP-supplied power cord is provided for each switch power supply. To prevent electric shock when connecting the switch to primary facility power, use only the supplied power cord(s), and ensure the facility power receptacle is the correct type, supplies the required voltage, and is properly grounded.

2. Turn on both power switches at the rear of the unit. The unit powers on and performs power-on self-tests (POSTs).

NOTE: If two power cords are used for high availability, plug the cords into separate facility power circuits.

3. During POSTs:
   a. The green power (PWR) LED on the switch front panel illuminates.

b. The amber system error (ERR) LED on the switch front panel blinks momentarily while the switch is tested.

c. The green LEDs associated with the Ethernet port blink momentarily while the port is tested.

d. The green and amber LEDs associated with the ports blink momentarily while the ports are tested.

4. After successful POST completion, the green power (PWR) LED remains illuminated and all other LEDs extinguish.

5. If a POST error or other malfunction occurs, go to "MAP 0000: Start MAP" on page -7 to isolate the problem.

NOTE: When powering on the switch after removing and replacing a faulty FRU, the amber system error LED may remain illuminated. Clear the system error LED as part of the replacement procedure.

Power-Off Procedure

To power-off the switch:

1. Notify the customer the switch is to be powered off. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the switch and sets attached devices offline.

2. Set the switch offline ("Set Offline State" on page -38).

3. Turn off both power switches at the rear of the unit.

4. If servicing the switch, disconnect the power cord(s) from the input power module at the rear of the switch. This step is not required when performing a power cycle.

Reset or IPL the Switch

A switch reset using the IML button (at the switch front panel) or IPL (at the *Product Manager* application) are functionally equivalent. They:

- Perform partial power-on diagnostics, reset functional logic for the CTP card, and load firmware from FLASH memory to random-access memory (RAM) without powering off the switch.

- Reset the Ethernet local area network (LAN) interface, causing the connection to the HAFM server to drop momentarily until the connection automatically recovers.
- Automatically enable changes to an active zone configuration.
- Keep all configured fabric logins, name server registrations, and operating parameters intact.
- Automatically set the switch online. The blocked state of each Fibre Channel port remains intact.

NOTE: A switch reset or IPL should be performed only if a CTP failure is indicated. Do not reset or IPL the switch unless directed to do so by a procedural step or the next level of support.

Reset the Switch

Resetting the switch with the IML button causes the switch to perform an initial program load (IML) that takes approximately 30 seconds.

To reset the switch:

1. At the switch front panel, press and hold the IML button for approximately three seconds.
2. During the reset, the switch-to-HAFM server Ethernet link drops momentarily and the following occurs at the *Product Manager* application:
   - — As the network connection drops, the **Status** table turns yellow, the **Status** field displays `No Link`, and the **State** field displays a reason message.
   - — The alert panel at the bottom of the navigation control panel displays a grey square, indicating switch status is unknown.
   - — Illustrated FRUs (SFPs, fans, and power supplies) in the **Hardware View** disappear, and appear again as the connection is re-established.

IPL the Switch

To IPL the switch:

1. At the HAFM server, open the *HAFM* application. The **Product View** displays.
2. Select the icon representing the switch to be IPled. The **Hardware View** for the selected switch displays.
3. At the navigation control panel, select **IPL** from the **Maintenance** menu. The **Information** dialog box displays.

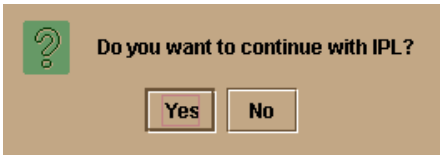


Figure 3–20: Information dialog box

4. Click **Yes** to IPL the switch. During the IPL, the switch-to-HAFM server Ethernet link drops momentarily and the following occur at the *Product Manager* application:
   - — As the network connection drops, the **Status** table turns yellow, the **Status** field displays `No Link`, and the **State** field displays a reason message.
   - — The alert panel at the bottom of the navigation control panel displays a grey square, indicating switch status is unknown.
   - — Illustrated FRUs (SFPs, fans, and power supplies) in the **Hardware View** disappear, and appear again as the connection is re-established.

Set the Switch Online or Offline

This section describes procedures to set the switch online or offline. These operating states are described as follows:

- **Online —** when the switch is set online, an attached device can log in to the switch if the port is not blocked. Attached devices can communicate with each other if they are configured in the same zone.
- **Offline —** when the switch is set offline, all switch ports are set offline. The switch transmits the offline sequence (OLS) to attached devices, and the devices cannot log in to the switch.

NOTE: When the switch is set offline, the operation of attached Fibre Channel devices is disrupted. Do not set the switch offline unless directed to do so by a procedural step or the next level of support.

Set Online State

To set the switch online:

1. At the HAFM server, open the *HAFM* application. The **Product View** displays.
2. Select the icon representing the switch to be set online. The **Hardware View** for the selected switch displays.

3. At the navigation control panel, select **Set Online State** from the **Maintenance** menu. If the switch is offline, the **Set Online State** dialog box displays, indicating the state is `OFFLINE`.

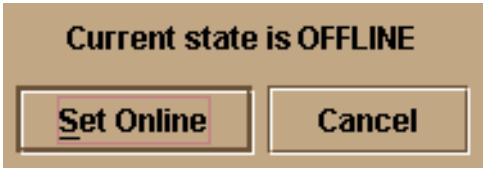


Figure 3–21: Online State dialog box

4. Click **Set Online**. A warning dialog box displays, indicating the switch is to be set online.
5. Click **OK**. As the switch comes online, inspect the *Product Manager* application. The **State** field of the **Status** table displays `Online`.

Set Offline State

To set the switch offline:

1. Notify the customer the switch is to be set offline. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the switch and sets attached devices offline.
2. At the HAFM server, open the *HAFM* application. The **Product View** displays.
3. Select the icon representing the switch to be set offline. The **Hardware View** for the selected switch displays.
4. At the navigation control panel, select **Set Online State** from the **Maintenance** menu. If the switch is online, the **Set Online State** dialog box displays, indicating the state is `ONLINE`.

5. Click **Set Offline**. A warning dialog box displays, indicating the switch is to be set offline.

6. Click **OK**. As the switch goes offline, inspect the *Product Manager* application. The **State** field of the **Status** table displays OFFLINE.

Block and Unblock Ports

This section describes procedures to block or unblock the switch ports. When a port is blocked, the port is automatically set offline. When a port is unblocked, the port is automatically set online.

NOTE: When a port is blocked, the operation of an attached Fibre Channel device is disrupted. Do not block a port unless directed to do so by a procedural step or the next level of support.

Block a Port

To block a port:

1. Notify the customer the port is to be blocked. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port.
2. At the HAFM server, open the *HAFM* application. The **Product View** displays.
3. Select the icon representing the switch with the port to be blocked. The **Hardware View** for the selected switch displays.
4. Move the pointer over the port and right-click the mouse to open a list of menus.
5. Select **Block Port**. The **Block Port *n*** dialog box displays (where *n* is the port number).

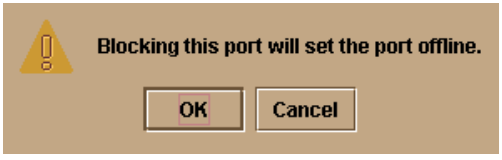


Figure 3–22: Block Port *n* dialog box

6. Click **OK**. The following occur to indicate the port is blocked (and offline):
   - The emulated green LED associated with the port extinguishes at the **Hardware View**.
   - The green LED associated with the port extinguishes at the switch.
   - A check mark displays in the check box adjacent to the **Block Port** menu.

Unblock a Port

To unblock a port:

1. At the HAFM server, open the *HAFM* application. The **Product View** displays.
2. Select the icon representing the switch with the port to be unblocked. The **Hardware View** for the selected switch displays.
3. Move the pointer over the port and right-click the mouse to open a list of menus options.
4. Select **Block Port**. Note the check mark in the box adjacent to the menu item, indicating the port is blocked. The **Unblock Port *n*** dialog box displays (where *n* is the port number).

Figure 3–23: Unblock Port *n* dialog box

5. Click **OK**. The following occur to indicate the port is unblocked (and online):
   - The emulated green LED associated with the port illuminates at the **Hardware View**.
   - The green LED associated with the port illuminates at the switch.
   - The check box adjacent to the **Block Port** menu option becomes blank.

Manage Firmware Versions

Firmware is the internal operating code stored on the switch's CTP card. Up to eight versions can be stored on the HAFM server hard drive and made available for download to a switch. Service personnel can perform the following firmware management tasks:

- Determine the firmware version active on a switch.
- Add to and maintain a library of up to eight firmware versions on the HAFM server hard drive.
- Modify a firmware description stored on the HAFM server hard drive.

- Delete a firmware version from the HAFM server hard drive.
- Download a firmware version to a selected switch.

Determine a Switch Firmware Version

To determine a switch firmware version:

1. At the HAFM server, open the *HAFM* application. The **Product View** displays.
2. Select the icon representing the switch to be inspected for firmware version. The **Hardware View** for the selected switch displays.
3. At the navigation control panel, select **Firmware Library** from the **Maintenance** menu. The **Firmware Library** dialog box displays.

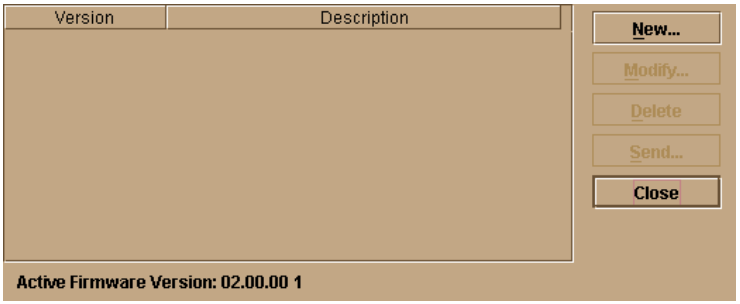


Figure 3–24: Firmware Library dialog box

4. The firmware version displays at the lower left corner of the dialog box in `XX.YY.ZZ` format, where `XX` is the version level, `YY` is the release level, and `ZZ` is the patch level.
5. Click **Close** to return to the **Hardware View**.

Add a Firmware Version

The firmware version shipped with the switch is provided on the Edge Switch 2/32 documentation kit CD. Subsequent firmware versions for upgrading the switch are provided to customers through the HP website.

NOTE: When adding a firmware version, follow all the instructions in the release notes that accompany the firmware version. This information supplements information in this general procedure.

To add a switch firmware version to the library stored on the HAFM server hard drive:

1. Obtain the new firmware version from the HP website:

NOTE: The following path is subject to change.

   a. At the HAFM server or other personal computer (PC) with Internet access, open the HP website. The uniform resource locator (URL) is:

   http://thenew.hp.com/country/us/eng/support.html

NOTE: If required, obtain the customer-specific member name and password from the customer or next level of support.

   b. Follow links to HAFM software.

   c. Click the Edge Switch 2/32 Firmware Version `XX.YY.ZZ` entry, where `XX.YY.ZZ` is the desired version. The **Windows Save As** dialog box displays.

   d. Ensure the correct directory path is specified at the **Save in** field and the correct file is specified in the **File name** field. Click **Save**. The new firmware version is downloaded and saved to the HAFM server or PC hard drive.

   e. If the new firmware version was downloaded to a PC (not the HAFM server), transfer the firmware version file to the HAFM server by diskette or other electronic means.

2. At the HAFM server, open the *HAFM* application. The **Product View** displays.

3. Select the icon representing the switch for which a firmware version is to be added. The **Hardware View** for the selected switch displays.

4. At the navigation control panel, select **Firmware Library** from the **Maintenance** menu. The **Firmware Library** dialog box displays.

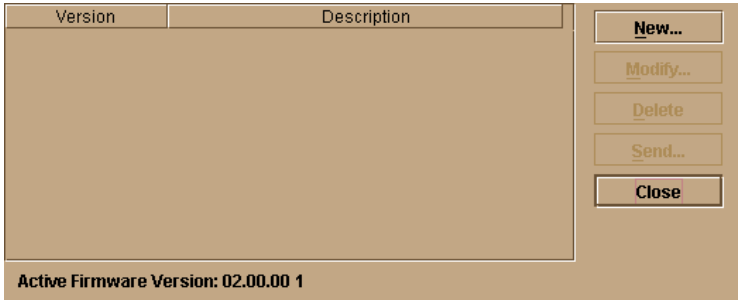


Figure 3–25: Firmware Library dialog box

5. Click **New**. The **New Firmware Version** dialog box displays.

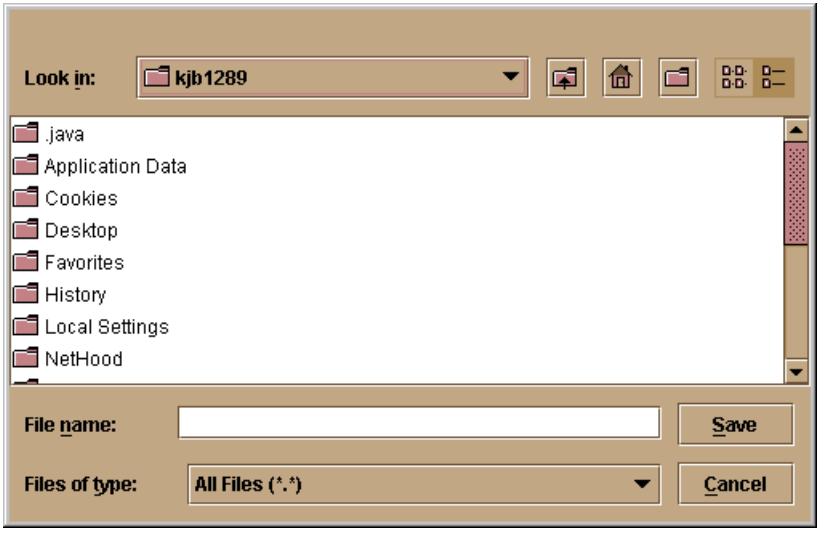


Figure 3–26: New Firmware Version dialog box

6. Select the desired firmware version file (downloaded in step 1) from the HAFM server CD-ROM or hard drive. Ensure the correct directory path and filename display in the **File name** field and click **Save**. The **New Firmware Description** dialog box displays.

Figure 3–27: New Firmware Description dialog box

7. Enter a description (up to 24 characters) for the new firmware version and click **OK**. The description should include the installation date and text that uniquely identify the firmware version.
8. A **Transfer Complete** message box displays indicating the new firmware version is stored on the HAFM server hard drive. Click **Close** to close the message box.

9. The new firmware version and associated description display in the **Firmware Library** dialog box. Click **Close** to close the dialog box and return to the *Product Manager* application.
10. To send the firmware version to a switch, refer to "Download a Firmware Version to a Switch" on page 3-46.

Modify a Firmware Version Description

To modify the description of a switch firmware version in the library stored on the HAFM server hard drive:

1. At the HAFM server, open the *HAFM* application. The **Product View** displays.
2. Select the icon representing the switch for which a firmware version is to be modified. The **Hardware View** for the selected switch displays.
3. At the navigation control panel, select **Firmware Library** from the **Maintenance** menu. The **Firmware Library** dialog box displays.

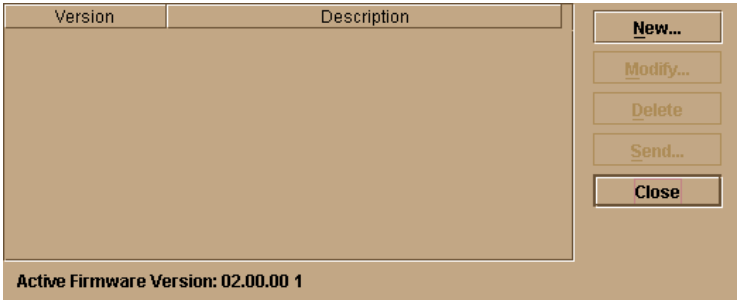


Figure 3–28: Firmware Library dialog box

4. Select the firmware version to be modified and click **Modify**. The **Modify Firmware Description** dialog box displays.

Figure 3–29: Modify Firmware Description dialog box

5. Enter a modified description (up to 24 characters) for the firmware version and click **OK**. The description should include the installation date and text that uniquely identify the firmware version.
6. The new description for the firmware version displays in the **Firmware Library** dialog box. Click **Close** to close the dialog box and return to the *Product Manager* application.

Delete a Firmware Version

To delete an switch firmware version from the library stored on the HAFM server hard drive:

1. At the HAFM server, open the *HAFM* application. The **Product View** displays.
2. Select the icon representing the switch from which the firmware version is to be deleted. The **Hardware View** for the selected switch displays.
3. At the navigation control panel, select **Firmware Library** from the **Maintenance** menu. The **Firmware Library** dialog box displays.

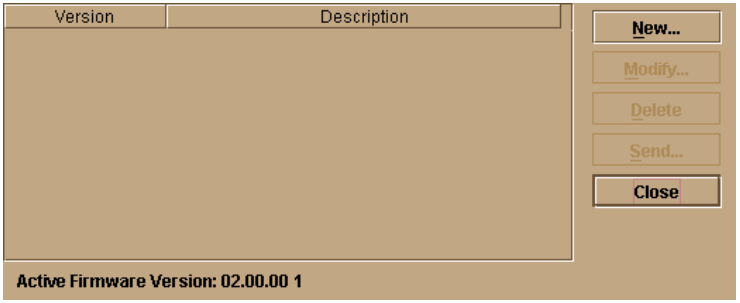


Figure 3–30: Firmware Library dialog box

4. Select the firmware version to be deleted and click **Delete**. A confirmation dialog box displays.
5. Click **OK**. The selected firmware version is deleted from the **Firmware Library** dialog box.
6. Click **Close** to close the dialog box and return to the *Product Manager* application.

Download a Firmware Version to a Switch

This procedure downloads a selected firmware version from the HAFM server library to a switch managed by the open instance of the *Product Manager* application.

NOTE: When downloading a firmware version, follow all procedural information in the release notes or EC instructions that accompany the firmware version. This information supplements information in this general procedure.

To download a firmware version to a switch:

1. Notify the customer that a firmware version is to be downloaded to the switch. The switch resets during the firmware download, causing Fibre Channel links to momentarily drop and attached devices to log out and log back in. Data frames lost during switch reset must be retransmitted.
2. At the HAFM server, open the *HAFM* application. The **Product View** displays.
3. Before downloading firmware version XX.YY.ZZ to a switch, ensure version XX.YY.ZZ or higher of the *HAFM* application is running on the HAFM server.
   a. Select **About** from the **Help** menu. The **About** dialog box displays the *HAFM* application version. Click **OK** to close the dialog box.
   b. If required, install the correct version of the *HAFM* application ("Install or Upgrade Software" on page 3-51).
4. Select the icon representing the switch for which a firmware version is to be downloaded. The **Hardware View** for the selected switch displays.
5. As a precaution to preserve switch configuration information, perform the data collection procedure ("Collecting Maintenance Data" on page 3-32).
6. At the navigation control panel, select **Firmware Library** from the **Maintenance** menu. The **Firmware Library** dialog box displays.

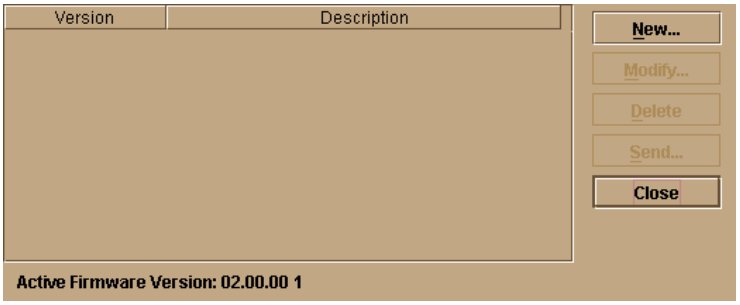


Figure 3–31: Firmware Library dialog box

7. Select the firmware version to be downloaded and click **Send**. The send function verifies existence of certain switch conditions before the download begins. If an error occurs, a message displays indicating the problem must be fixed before the firmware download. Conditions that terminate the process include:

   — The firmware version is being installed to the switch by another user.

   — The switch-to-HAFM server link fails or times out.

   If a problem occurs and a corresponding message displays, go to "MAP 0000: Start MAP" on page 2-7 to isolate the problem. If no error occurs, the **Send Firmware** confirmation box displays.

Figure 3–32: Send Firmware confirmation box

8. Click **Yes**. The **Send Firmware** dialog box displays.

   As the download begins, a `Sending Files` message displays at the top of the dialog box. This message remains for a few moments as a progress bar travels across the dialog box to show percent completion of the download. As the download progresses, a `Writing data to FLASH` message displays. This message remains as the progress bar continues to travel across the dialog box. The

bar progresses to 100% when the last file is transmitted to the CTP card. The switch then performs an IPL, during which the switch-to-HAFM server link drops momentarily and the following occur at the *Product Manager* application:

— As the network connection drops, the **Status** table turns yellow, the **Status** field displays `No Link`, and the **State** field displays a reason message.

— The alert panel at the bottom of the navigation control panel displays a grey square, indicating switch status is unknown.

— Illustrated FRUs in the **Hardware View** disappear, and appear again as the connection is re-established.

After the IPL, a `Send firmware complete` message displays as shown below.

Figure 3–33: Send firmware complete message

9. Click **Close** to close the dialog box.
10. Click **Close** to close the **Firmware Library** dialog box and return to the **Hardware View**.

Manage Configuration Data

The *Product Manager* application provides maintenance options to back up, restore, or reset the configuration file stored in nonvolatile random-access memory (NV-RAM) on the switch CTP card. Configuration data in the file include:

- Identification data (switch name, description, and location).
- Port configuration data (port names, blocked states, and port validation, auto-LIP, and LIN alert configurations).
- Operating parameters (loop mode, error detect time out value (*E_D_TOV*), resource allocation time out value (*R_A_TOV*), and preferred domain ID).

- Simple network management protocol (SNMP) configuration information, including trap recipients, community names, and write authorizations.
- Zoning configuration information, including the active zone set and default zone state.

NOTE: The switch must be set offline prior to restoring or resetting the configuration file.

Back Up the Configuration

NOTE: The ability to back up configuration data may not exist if the user has a customer-supplied server platform for the *HAFM* application. The server platform just have Iomega® QuikSync and a Zip drive.

To back up the switch configuration file to the HAFM server (c:\HafmData):

1. At the HAFM server, open the *HAFM* application. The **Product View** displays.
2. Select the icon representing the switch for which a configuration file is to be backed up. The **Hardware View** for the selected switch displays.
3. At the navigation control panel, select **Backup & Restore Configuration** from the **Maintenance** menu. The **Backup and Restore Configuration** dialog box displays.

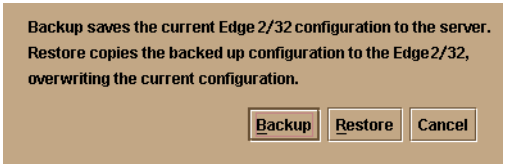

Backup saves the current Edge 2/32 configuration to the server.
Restore copies the backed up configuration to the Edge 2/32,
overwriting the current configuration.
Backup
Restore
Cancel

Figure 3–34: Backup and Restore Configuration dialog box

4. Click **Backup**. When the backup process finishes, the **Backup Complete** dialog box displays.

Figure 3–35: Backup Complete dialog box

5. Click **OK** to close the dialog box and return to the **Hardware View**.

Restore the Configuration

To restore the switch configuration file from the HAFM server:

1. Notify the customer that the switch is to be set offline. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the switch and sets attached devices offline.
2. Set the switch offline ("Set Offline State" on page 3-38).
3. At the HAFM server, open the *HAFM* application. The **Product View** displays.
4. Select the icon representing the switch for which a configuration file is to be restored. The **Hardware View** for the selected switch displays.
5. At the navigation control panel, select **Backup & Restore Configuration** from the **Maintenance** menu. The **Backup and Restore Configuration** dialog box displays.

Backup saves the current Edge-32 configuration to the server.
Restore copies the backed up configuration to the Edge-32,
overwriting the current configuration.
Backup
Restore
Cancel

Figure 3–36: Backup and Restore Configuration dialog box

6. Click **Restore**. A warning message box displays.

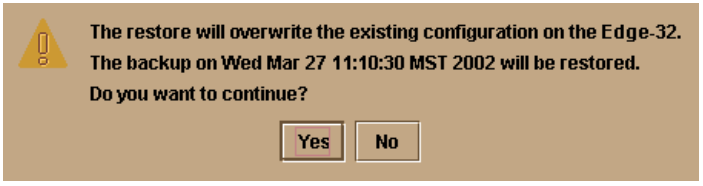

The restore will overwrite the existing configuration on the Edge-32.
The backup on Wed Mar 27 11:10:30 MST 2002 will be restored.
Do you want to continue?
Yes
No

Figure 3–37: Warning message box

7. Click **Yes**. When the restore process finishes, the **Restore Complete** dialog box displays.

Figure 3–38: Restore Complete dialog box

8. Click **OK** to close the dialog box and return to the **Hardware View**.

Reset Configuration Data

NOTE: This procedure resets the switch IP address to the default of 10.1.1.10 and may disrupt server-to-switch communication.

To reset the switch data to the factory default settings:

1. Notify the customer the switch is to be set offline. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the switch and sets attached devices offline.
2. Set the switch offline ("Set Offline State" on page 3-38).
3. At the HAFM server, open the *HAFM* application. The **Product View** displays.
4. Select the icon representing the switch for which a configuration file is to be reset to factory default settings. The **Hardware View** for the selected switch displays.
5. At the navigation control panel, select **Reset Configuration** from the **Maintenance** menu. The **Reset Configuration** dialog box displays.
6. Click **Reset**. When the reset process finishes, the dialog box closes and the application returns to the **Hardware View**.

Install or Upgrade Software

This section describes the procedure to install or upgrade the *HAFM* application to the HAFM server. The *HAFM* application includes the switch Product Manager and *HAFM Services* applications.

The *HAFM* application shipped with the switch is provided on the *HAFM* applications CD-ROM. Subsequent software versions for upgrading the switch are provided to customers through the *HAFM* applications CD-ROM or through HP's home page.

NOTE: When installing or upgrading a software version, follow all procedural information in the release notes or EC instructions that accompany the software version. This information supplements information in this general procedure.

To install or upgrade the *HAFM* application and associated applications to the HAFM server:

1. Log out of all *HAFM* application sessions (local and remote) and exit the *HAFM* application.
2. To obtain the new software version from the *HAFM* applications CD-ROM, go to step 4.
3. To obtain the new software version from HP's home page:
   a. At the HAFM server or other personal computer (PC) with internet access, open the HP home page. The URL is http://www.hewlettpackard.com.
   b. Move the pointer over Services at the top of the home page to open a list of menu selections, then click the **Support Login** selection. The **Hewlett Packard Central Site** page displays.
   c. Type a member name and password (both are case sensitive) and click **Sign In**. The **Hewlett Packard Central Site File Library** page displays.

      If required, obtain the customer-specific member name and password from the customer or next level of support.
   d. Click the **Microcode Downloads** folder. A list of software available for download displays at the right side of the window.

NOTE: If required, obtain the customer-specific member name and password from the customer or next level of support.

   e. Click the appropriate HAFM server Version `XX.YY.ZZ` entry, where `XX.YY.ZZ` is the desired version. A **File Download** dialog box displays.
   f. Select **Save this program to disk** and click **OK**.
   g. Ensure the correct directory path (c:\HafmData) is specified at the **Save as** dialog box, and the correct file is specified in the **File name** field. Click **Save**. The new software version executable file is downloaded and saved to the HAFM server or PC hard drive.
   h. If the executable file was downloaded to a PC (not the HAFM server), transfer the firmware version file to the HAFM server by diskette or other electronic means.
   i. Go to step 5.

4. Insert the *HAFM* applications CD-ROM into the CD-ROM drive of the HAFM server.
5. At the HAFM server, click **Start** at the Windows task bar. The **Windows Workstation** menu displays.
6. At the **Windows Workstation** menu, select **Run**. The **Run** dialog box displays.

Type the name of a program, folder, or document, and Windows will open it for you.
Open:
Run in Separate Memory Space
OK
Cancel
Browse...

Figure 3–39: Run dialog box

7. At the **Run** dialog box, select the directory path (hard drive or CD-ROM drive) and filename of the executable file (*HAFM_ServerInstall.exe*) using the **Browse** button. The directory path and filename display in the **Open** field.
8. Click **OK**. A series of message boxes display as the *InstallAnywhere* third-party application prepares to install the *HAFM* application software, followed by the **HAFM** dialog box.

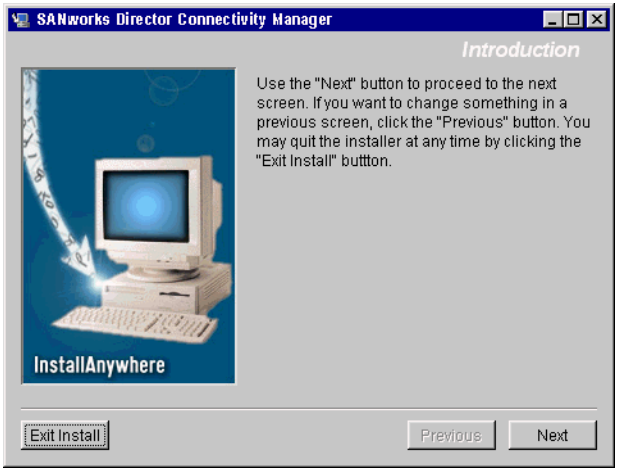

SANworks Director Connectivity Manager
Introduction
Use the "Next" button to proceed to the next screen. If you want to change something in a previous screen, click the "Previous" button. You may quit the installer at any time by clicking the "Exit Install" buttton.
InstallAnywhere
Exit Install
Previous
Next

Figure 3–40: HAFM dialog box

9. Follow the online instructions for the InstallAnywhere program. Click **Next**, **Install**, or **Done** as appropriate.
10. Power off and reboot the HAFM server PC.
    a. Simultaneously press **Ctrl**, **Alt**, and **Delete** to display the **Windows Logon Information** dialog box.
    b. Type a user name and password and click **OK**. The Windows desktop displays.

NOTE: If required, obtain the user name and password from the customer or next level of support.

11. The *HAFM* application automatically opens. At the HAFM splash screen, enter a user name, password, and HAFM server name (all are case sensitive), and click **Login**. The application opens and the **Product View** displays.

NOTE: If required, obtain the user name, password, and HAFM server name from the customer or next level of support.

4

FRU Removal and Replacement

This chapter describes the removal and replacement procedures (RRPs) for the HP StorageWorks Edge Switch 2/32 (Edge Switch 2/32) field-replaceable units (FRUs). Do not remove a FRU until a failure is isolated to that FRU. If fault isolation was not performed, see MAP 0000: Start MAP on page 2–7.

Remove and Replace FRUs

This section describes procedures to remove and replace (RRPJ) concurrent switch FRUs. A screwdriver is required to remove and replace the power supplies. No tools are required to remove and replace the other FRUs. All FRUs are removed and replaced while the switch is powered on and operational (concurrent FRUs). See Chapter 5, Illustrated Parts Breakdown for FRU locations and part numbers.

FRUs

Table 4–1 lists the FRUs and electrostatic discharge (ESD) precaution requirements (yes or no) for each FRU.

Table 4–1: ESD Requirements

FRU Name	ESD Precaution Requirement
SFP LC transceiver	No
Power supply	No
Cooling fan	No

Procedural Notes

Note the following:

1. Read the removal and replacement procedures (RRPs) for that FRU before removing the FRU.
2. Follow all **WARNING** and **CAUTION** statements and statements in the preface of this manual.
3. After completing a FRU replacement, clear the event code reporting the failure and the event code reporting the recovery from the switch Event Log (at the HAFM server). Extinguish the amber system error (**ERR**) light-emitting diode (LED) at the switch front panel.

RRP: SFP Transceiver

Use the following procedures to remove and replace an SFP transceiver from a port. No tools are required.

Removal

To remove an SFP:

1. Identify the defective port from the illuminated amber LED at the switch or failure information at the HAFM server's **Hardware View**.
2. Notify the customer the port will be blocked. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port and sets the attached device offline.
3. Block communication to the defective port (refer to Block a Port on page 3–39).
4. Disconnect the fiber-optic jumper cable from the SFP:
   a. Pull the keyed subscriber connector (LC) free from the SFP.
   b. Place a protective cap over the cable connector.
5. If the SFP was not manufactured by IBM Corporation, go to step 6. Remove an IBM-manufactured SFP from the chassis:
   a. Flip the wire bale at the bottom of the SFP upward 90 degrees.
   b. Use the wire bale as a handle to pull the SFP out of the chassis.

6. Remove a non-IBM SFP from the chassis:
   a. Simultaneously squeeze the metal latches on the sides of the SFP to disengage the SFP from the port receptacle.
   b. Pull the SFP out of the chassis.
7. At the HAFM server's **Hardware View**, select **Event Log** from the **Logs** icon. The Event Log displays. Ensure the following event code displays in the log:
   — **510 —** SFP hot-insertion initiated.

Replacement

To install an SFP in a switch port:

1. Remove the replacement SFP from its shipping container.
2. If the SFP was not manufactured by IBM Corporation, go to step 3. Insert an IBM-manufactured SFP into the port receptacle:
   a. Ensure the IBM label is at the top, and the alignment groove is at the bottom.
   b. Verify the SFP is aligned in the receptacle, then slide it forward until it seats firmly.
   c. Flip the wire bale (handle) of the SFP downward 90 degrees.
3. Insert a non-IBM SFP into the G_Port receptacle:
   a. Ensure the label that identifies the OEM of the SFP is at the top, and the alignment groove is at the bottom.
   b. Verify the SFP is aligned in the receptacle, then slide it forward until it seats.
4. Perform an external loopback test for the port (refer to External Loopback Test on page 3–28). If the test fails, go to MAP 0000: Start MAP on page 2–7 to isolate the problem.
5. Connect the fiber-optic jumper cable to the port SFP:
   a. Remove the protective cap from the cable connector. Store the cap for safekeeping.
   b. Clean the cable and SFP connectors (refer to Clean Fiber-Optic Components on page 3–33).
   c. Insert the keyed LC cable connector into the port SFP.

d. Verify that the amber LED adjacent to the port is extinguished.

6. At the HAFM server's **Hardware View**, select **Event Log** from the **Logs** icon. The Event Log displays. Ensure the following event code displays in the log:

   — **513 —** SFP hot-removal completed.

   If an event code **513** does not display in the log, go to MAP 0000: Start MAP on page 2–7 to isolate the problem.

7. At the HAFM server's **Hardware View**:

   a. Ensure no alert symbols display that indicate a failure (yellow triangle or red diamond).

   b. Click the port graphic representing the replacement SFP to open the **Port Properties** dialog box. Verify that port information (port number, port name, operational state, and port technology) is correct.

   If a problem is indicated, go to MAP 0000: Start MAP on page 2–7 to isolate the problem.

8. Restore communication to the port and set the port online as directed by the customer (refer to Unblock a Port on page 3–40).

9. Perform the data collection procedure (refer to Collecting Maintenance Data on page 3–32).

10. Clear the switch's system error (**ERR**) LED:

    a. At the HAFM server's **Hardware View**, right-click the front panel bezel graphic (away from a FRU) to open a pop-up menu.

    b. Click the **Clear System Error Light** menu selection.

RRP: Power Supply

Use the following procedures to remove or replace a power supply from the rear of the switch. No tools are required.

Removal

To remove a power supply:

1. Identify the defective power supply from the extinguished green LED at the switch or failure information at the HAFM server's **Hardware View**.

2. Turn off the power switch on the power supply.
3. Disconnect the AC power cord from the power supply.
4. Rotate the power lockout lever to the right to expose the black plastic latch lever.
5. Pull the latch lever down to the horizontal position.

   The power supply will disengage and back out about 1/4 inch when the lever is horizontal.
6. Use the latch lever to pull the power supply out of the chassis. Support the power supply as it exits the chassis.

WARNING: To prevent electric shock, do not reach into nonvisible areas of a switch while the switch is connected to primary facility power.

Replacement

To replace a power supply:

1. Remove the replacement power supply from its shipping container.
2. Inspect the rear of the power supply for bent or broken connector pins. If any pins are damaged, obtain a new power supply.
3. Ensure that the power switch on the power supply is turned off, the power lockout lever is rotated to the right, covering the AC connector, and the black plastic latch lever is completely down in the horizontal position.
4. Insert the power supply into the chassis until it stops.
5. Raise the black plastic latch lever to the vertical position.

   The power supply cams into its seated position in the chassis.
6. Rotate the power lockout lever to the left to cover the plastic lever and expose the AC connector.
7. Verifying that the power switch is off, connect the AC power cord to the power supply and to a facility power source.
8. Turn on the power switch.

9. Inspect the power supply to ensure that the green LED is illuminated. If the green LED is extinguished, go to MAP 0000: Start MAP on page 2–7 to isolate the problem.
10. At the HAFM server's **Hardware View**, select **Event Log** from the **Logs** icon. The Event Log displays. Ensure the following event codes display in the log:
    - **203 —** Power supply AC voltage recovery.
    - **204 —** Power supply DC voltage recovery.
11. At the HAFM server's **Hardware View**, observe the power supply graphic and ensure no alert symbols display that indicate a failure (yellow triangle or red diamond). If a problem is indicated, go to MAP 0000: Start MAP on page 2–7 to isolate the problem.
12. Perform the data collection procedure (refer to Collecting Maintenance Data on page 3–32).
13. Clear the switch system error (**ERR**) LED:
    a. At the HAFM server's **Hardware View**, right-click the front panel bezel graphic (away from a FRU) to open a pop-up menu.
    b. Click the **Clear System Error Light** menu selection.

RRP: Cooling Fan

Use the following procedures to remove or replace a cooling fan from the rear of the switch. No tools are required.

Removal

To remove a cooling fan:

1. Identify the defective cooling fan from the illuminated amber LED on the fan or failure information at the HAFM server's **Hardware View**.
2. Loosen the fan retaining screw in the upper right corner of the fan. This is a captive screw that will remain in the fan assembly.
3. Grasp the fan handle and pull the fan FRU out of the chassis.

Replacement

To replace a cooling fan:

1. Remove the replacement cooling fan FRU from its shipping container.
2. Inspect the rear of the fan for bent or broken connector pins. If any pins are damaged, obtain a new fan.
3. Position the fan FRU with its retaining screw at the upper right corner (the fan cannot be inserted in any other position).
4. Push the fan FRU into the chassis to engage the connector pins until the fan faceplate is flush with the chassis.
5. Engage the screw threads and lightly tighten the screw. Over-tightening the screw may damage the FRU or chassis.
6. Inspect the fan FRU to ensure that the amber LED is extinguished. If the amber LED is illuminated, go to MAP 0000: Start MAP on page 2–7 to isolate the problem.
7. At the HAFM server's **Hardware View**, select **Event Log** from the **Logs** icon. The Event Log displays. Ensure one of the following event codes displays in the log:
   - **310 to 315 —** *N*th cooling fan has recovered, where *N* is first to fourth (fan).
8. At the HAFM server's **Hardware View**, observe the fan graphic and ensure no alert symbols display that indicate a failure (yellow triangle or red diamond). If a problem is indicated, go to MAP 0000: Start MAP on page 2–7 to isolate the problem.
9. Perform the data collection procedure (refer to Collecting Maintenance Data on page 3–32).
10. Clear the switch system error (**ERR**) LED:
    a. At the HAFM server's **Hardware View**, right-click the front panel bezel graphic (away from a FRU) to open a pop-up menu.
    b. Click the **Clear System Error Light** menu selection.

RRP: CTP Card — Switch Replacement

Some event codes indicate a CTP card failure, as do some diagnostic paths through MAPs. The CTP card is not a FRU, and cannot be replaced. CTP card failure requires replacement of the entire switch. If the failed switch provides a critical singular link in the fabric, and that link is still operating, it may be necessary to schedule down-time for this replacement.

Replacing a Failed Switch

NOTE: This procedure assumes that the new switch will be installed in the same location as the failed switch and will be configured the same as the failed switch.

Replacing a failed switch in an existing fabric requires the following tasks be done, in order:

- Note the following information for the failed switch: domain number, contact name, `BB_Credit`, `R_A_TOV`, `E_D_TOV`, Preferred Domain ID, Switch Priority, and Rerouting Delay, and the configuration of the ports, SNMP traps, CLI, and EWS.
- Remove the failed switch:
  - — Ensure the failed switch is no longer carrying traffic.

    Set the switch offline.
  - — Using HAFM, remove the switch from the fabric.

    Delete the switch from the fabric, using the HAFM **Product View**.
  - — Physically disconnect and remove the switch from the mounting location.
- Set up the new switch to operate in the fabric:
  - — Physically mount the new switch in the mounting location.
  - — Verify that the new switch powers up successfully.

    After successful power-on-self-tests, the green PWR LED remains on and all other front panel LEDs extinguish.
  - — Set the switch to operate on the LAN:

    1. Connect a maintenance terminal to the 9-pin maintenance port.

    2. Using Hyperterminal, connect to the Edge Switch 2/32.

    3. Enter the default password (password).

4. At the C: prompt, type `ipconfig` and press **Enter**.

5. Set the IP address, subnet mask, and gateway address the same as the failed switch and press **Enter**.

6. Close Hyperterminal and disconnect the maintenance terminal.

— Connect the switch to the LAN.

— Configure the switch for the *HAFM* application:

1. Right-click in a blank area of the HAFM **Product View** and select **New**.

2. Type the IP address of the switch in the **New Product** dialog box.

3. Select the correct product type from the **Product Type** field and click **OK**. A new icon will display on the **Product View**.

— Configure the switch identification:

1. Click the new icon to open the **Hardware View** and click the **Configure** icon.

2. Select identification from the **Configure** menu.

3. In the **Configure Identification** dialog box, type the name, description, location, and contact the same as the failed switch.

— Configure operating mode:

1. Set the switch offline.

2. At the **Hardware View**, select operating parameters from the **Configure** menu.

3. Set *BB_Credit*, *R_A_TOV*, *E_D_TOV*, Preferred Domain ID, Switch Priority, and Rerouting Delay the same as the failed switch, and click **Activate**.

— Verify the firmware version:

1. At the **Hardware View**, select firmware library from the **Maintenance** icon and verify that the firmware version is the same as that running on the existing fabric. The active version is displayed at the bottom of the display. To upgrade/download the active version, select the correct version and select **SEND**. The firmware will load, perhaps taking up to 10 minutes.

— Configure the ports the same as the failed switch (select ports from the **Configure** menu).

— Configure SNMP traps, CLI, EWS the same as the failed switch.

— Set the date and time.

— Set zoning configuration:

1. At the HAFM **Product View**, select **Fabric**. Select the new switch icon, then **Zone Set** tab.

2. Verify that the active zoneset is the same active zoneset that is running on the fabric, and that the default zone is disabled.

- Add the switch to the fabric:

— Connect the fibre-optic cables to the switch ports.

— Set the switch online.

— Verify that the switch successfully joins the fabric.

5

Illustrated Parts Breakdown

This chapter provides an illustrated parts breakdown for the HP StorageWorks Edge Switch 2/32 field-replaceable units (FRUs). Exploded-view assembly drawings are provided for:

- Front-accessible FRUs.
- Rear-accessible FRUs.
- Miscellaneous parts.

Exploded-view illustrations portray the switch disassembly sequence. Illustrated FRUs are numerically keyed to associated tabular parts lists. The parts lists also include part numbers, descriptions, and quantities.

Front-Accessible FRUs

The front-accessible switch FRUs are illustrated and described in Figure 5–1 and Table 5–1. The table includes reference numbers to the figure, part numbers, descriptions, and quantities.

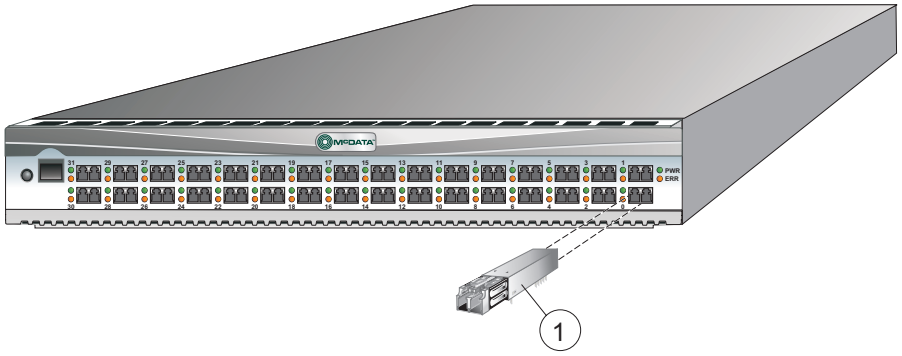


Figure 5–1: Front-Accessible FRUs

Table 5–1: Front-Accessible FRU Parts List

Ref.	Part Number	Description	Qty.
	292008-001	Base assembly, Edge Switch 2/32, without optics	Reference
❶	292003-001	Transceiver, optical, shortwave laser, 2.125 Gbps, 850 nm, LC (2 to 300 meters)	0 to 32
❶	292004-001	Transceiver, optical, longwave laser, 2.125 Gbps, 1300 nm, LC (up to 10 km)	0 to 32
❶		Transceiver, optical, extended longwave laser, 2.125 Gbps, 1300 nm, LC (up to 35 km)	0 to 32

Rear-Accessible FRUs

The FRUs and their part numbers differ between the two packaging systems for the switch. Use care when selecting a part number to order for replacement purposes to ensure that the part number matches the switch for which it is intended.

The rear-accessible switch FRUs are illustrated and described in Figure 5–2 and Table 5–2. The table includes reference numbers to the figure, part numbers, descriptions, and quantities.

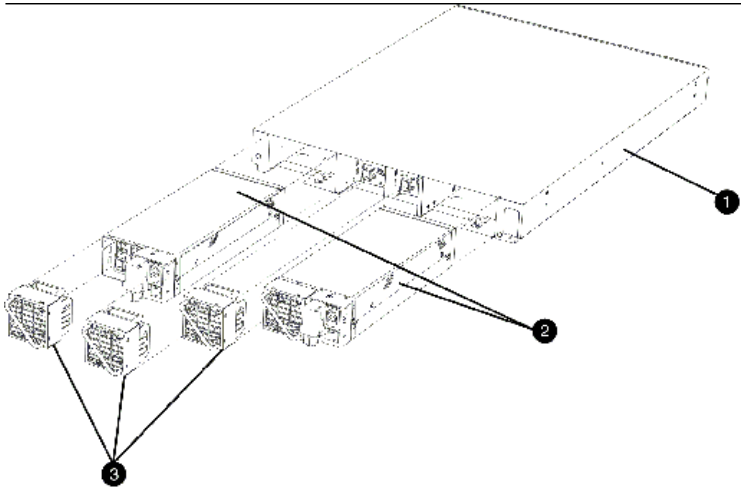


Figure 5–2: Rear-Accessible FRUs

Table 5–2: Rear-Accessible FRU Parts List

Ref.	Part Number	Description	Qty.
❶	292008-001	Base assembly, Edge Switch 2/32, without optics	Reference
❷	292012-001	Power supply assembly (includes one cooling fan, P/N 292010-001)	2
❸	292010-001	Fan, cooling	4

Miscellaneous Parts

Table 5–3 is a list of miscellaneous parts.

Table 5–3: Miscellaneous Parts

Ref.	Part Number	Description	Qty.
Ref	254138-001	Power cord, 120 VAC, United States	
Ref	258754-001	Power cord, AC, 5-15R	
Ref	254139-001	Power cord, AC Adapter/Jumper, 2.5 m	
Ref	258753-001	Adapter, ac, 100-240 VAC, autosense	
Ref	254143-001	Cable, Ethernet, 10 ft	
Ref	254144-001	Cable, null modem, 10 ft	
Ref	254145-001	Plug, loopback, shortwave	
Ref	254146-001	Plug, loopback, longwave	
Ref	258750-001	PC, laptop, without manuals	
Ref	254147-001	Rackmount kit, 9000 and 11000 series	
Ref	254148-001	Rackmount kit, M series	
Ref	254135-001	Screwdriver, with bit	

A

Messages

This appendix lists information and error messages that display in pop-up message boxes at the HP StorageWorks *High Availability Fabric Manager* (*HAFM*) application and HP StorageWorks *Edge Switch 2/32 Product Manager* applications.

The first section of the appendix lists *HAFM* application messages. The second section lists Product Manager messages. The text of each message is followed by a description and recommended course of action.

HAFM Application Messages

This section lists *HAFM* application information and error messages in alphabetical order.

Message	Description	Action
`A zone must have at least one zone member.`	When creating a new zone, one or more zone members must be added.	Add one or more zone members to the new zone.
`A zone set must have at least one zone.`	When creating a new zone set, one or more zones must be added.	Add one or more zones to the new zone set.
`All alias, zone, and zone set names must be unique.`	When creating a new alias, zone, or zone set, the name must be unique.	Choose a unique name for the new alias, zone, or zone set.
`All zone members are logged.`	Attempt was made to display all zone members not logged-in using the **Zone Set** tab, but all members are currently logged in.	Informational message.

Message	Description	Action
An HAFM application session is already active from this workstation.	Only one instance of the *HAFM* application is allowed to be open per remote workstation.	Close all but one of the *HAFM* application sessions.
Are you sure you want to delete this network address?	The currently selected network address will be deleted.	Click **Yes** to delete or **No** to cancel.
Are you sure you want to delete this nickname?	The selected nickname will be deleted from the list of nickname definitions.	Click **Yes** to delete the nickname or **No** to cancel the operation.
Are you sure you want to delete this product?	The selected product will be deleted from the list of product definitions.	Click **Yes** to delete the product or **No** to cancel the operation.
Are you sure you want to delete this user?	The selected user will be deleted from the list of user definitions.	Click **Yes** to delete the user or **No** to cancel the operation.
Are you sure you want to delete this zone?	The selected zone will be deleted from the zone library.	Click **Yes** to delete the zone or **No** to cancel the operation.
Are you sure you want to delete this zone set?	The selected zone set will be deleted from the zone library.	Click **Yes** to delete the zone set or **No** to cancel the operation.
Are you sure you want to overwrite this zone set?	The selected zone set will be overwritten in the zoning library.	Click **Yes** to overwrite or **No** to cancel.
Are you sure you want to remove all members from this zone?	All members will be deleted from the selected zone.	Click **Yes** to delete the members or **No** to cancel the operation.

Message	Description	Action
`Cannot add a switch to a zone.`	The device that you are attempting to add to the zone is a switch, which cannot be added to a zone.	Specify the port number or corresponding World Wide Name for the device you want to add to the zone.
`Cannot connect to HAFM server.`	The *HAFM* application at a remote workstation could not connect to the HAFM server.	Verify the HAFM server internet protocol (IP) address is valid.
`Cannot delete product.`	The selected product cannot be deleted.	Verify the HAFM server-to-product link is up. • If the link is up, the HAFM server may be busy. • Another Product Manager instance may be open. • The user may not have permission to delete the product.
`Cannot disable Fabric Binding while Enterprise Fabric Mode is active.`	User attempted to disable Fabric Binding through the **Fabric Binding** dialog box, but Enterprise Fabric Mode was enabled.	Disable Enterprise Fabric Mode through the **Enterprise Fabric Mode** dialog box in HAFM before disabling Fabric Binding.
`Cannot display route. All switches in route must be managed by the same server.`	You cannot show the route between devices that are attached to switches or directors managed by a different HAFM server.	Make sure devices named in **Show Routes** dialog box are attached to products managed by this HAFM server.

Message	Description	Action
Cannot display route. All switches in route must support routing.	You cannot show the route through a fabric that has switches or directors which do not support routing.	The route must contain only Director 2/64; or Edge Switch 2/16, and Edge Switch 2/32 switches.
Cannot display route. Device is not a member of a zone in the active zone set.	You cannot show the route for a device that is not a member of a zone in the active zone set. The source node that you have selected is not part of a zone in the active zone set.	Enable the default zone or activate the zone for the device before attempting to show the route.
Cannot display route. error 9.	An internal error has occurred while trying to view routes.	Contact the next level of support to report the problem.
Cannot display route. No active zone enabled.	You cannot show the route through a fabric with no active zone.	Enable the default zone or activate a zone set before attempting to show the route.
Cannot display route on a one switch fabric.	The user cannot show routes between end devices in a fabric when configuring Show Routes (**Fabrics** menu).	Error displays when attempting to show routes on a fabric with only one switch. Configure the Show Route option on a multiswitch fabric.
Cannot have spaces in field.	Spaces are not allowed as part of the entry for this field.	Delete spaces from the field entry.
Cannot modify a zone with an invalid name. Rename zone and try again.	A zone must have a valid name to be modified.	Assign a valid name to the zone, then click **Modify**.
Cannot modify a zone set with an invalid name. Rename zone set and try again.	A zone set must have a valid name to be modified.	Assign a valid name to the zone set, then click **Modify**.

Message	Description	Action
`Cannot modify product.`	The selected product cannot be modified.	Verify the HAFM server-to-product link is up. • If the link is up, the HAFM server may be busy. • Another Product Manager instance may be open. • The user may not have permission to modify the product.
`Cannot perform operation. Fabric is unknown.`	This message displays if no switches in the fabric are connected to the HAFM server.	Ensure at least one fabric-attached switch or director has an Ethernet connection to the HAFM server and retry the operation.
`Cannot perform operation. The list of attached nodes is unavailable.`	This message displays when attached nodes are unavailable and the user attempts to modify a zone or create a new zone.	Verify an attached node is available and retry the operation.
`Cannot retrieve current SNMP configuration.`	The current SNMP configuration could not be retrieved.	Try again. If the problem persists, contact the next level of support.
`Cannot save current SNMP configuration.`	The current SNMP configuration could not be saved.	Try again. If the problem persists, contact the next level of support.

Message	Description	Action
`Cannot set write authorization without defining a community name.`	An SNMP community name has not been configured.	Enter a valid community name in the **Configure SNMP** dialog box.
`Cannot show zoning library. No fabric exists.`	You cannot show the zoning library if no fabric exists. You must have identified a switch or director to HAFM for a fabric to exist.	Identify an existing switch or director to HAFM using the **New Product** dialog box.
`Click OK to remove all contents from log.`	This action deletes all contents from the selected log.	Click **OK** to delete the log contents or **Cancel** to cancel the operation.
`Could not export log to file.`	A log file input/output (I/O) error occurred and the file could not be saved to the specified destination. The disk may be full or write protected.	If the disk is full, use another disk. If the disk is write protected, change the write-protect properties or use another disk.
`Default zoning is not supported in Open Fabric Mode.`	A default zone cannot be enabled when the product is enabled for Open Fabric mode. Open Fabric mode does not support zone members defined by port numbers.	Redefine zone members by the WWN of attached devices.
`Device is not a member of a zone in the active zone set.`	The selected device is not a member of a zone in the active zone set and therefore cannot communicate with the other device in the route.	Enable the default zone or activate a zone set containing the member before attempting to show the route.
`Download complete. Click OK and start the HAFM.`	Download of the *HAFM* and *Product Manager* applications is complete.	Start the *HAFM* application to continue.

Message	Description	Action
`Duplicate community names require identical write authorizations.`	If configuring two communities with identical names, they must also have identical write authorizations.	Verify that both communities with the same name have the same write authorizations.
`Duplicate name in zoning configuration.`	Every name in the zoning library must be unique.	Modify (to make it unique) or delete the duplicate name.
`Duplicate nickname in nickname configuration.`	Duplicate nicknames cannot be configured.	Modify the selected nickname to make it unique.
`Duplicate World-Wide Name in nickname configuration.`	A world-wide name can be associated with only one nickname.	Modify (to make it unique) or delete the selected world-wide name.
`Duplicate zone in zone set configuration.`	More than one instance of a zone is defined in a zone set.	Delete one of the duplicate zones from the zone set.
`Duplicate zone member in zone configuration.`	More than one instance of a zone member is defined in a zone.	Delete one of the duplicate zone members from the zone.
`Enabling this zone set will replace the currently active zone set. Do you want to continue?`	Only one zone set can be active. By enabling the selected zone set, the current active zone set will be replaced.	Click **OK** to continue or **Cancel** to end the operation.
`Error creating zone.`	The *HAFM* application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.

Message	Description	Action
`Error creating zone set.`	The *HAFM* application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
`Error deleting zone.`	The *HAFM* application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
`Error deleting zone set.`	The *HAFM* application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
`Error reading log file.`	The *HAFM* application encountered an error while trying to read the log.	Try the operation again. If the problem persists, contact the next level of support.
`Error removing zone or zone member.`	The *HAFM* application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
`Error transferring files < message >.`	An error occurred while transferring files from the PC hard drive to the *HAFM* application. The message varies, depending on the problem.	Try the file transfer operation again. If the problem persists, contact the next level of support.
`Fabric Log will be lost once the fabric unpersists. Do you want to continue?`	When you unpersist a fabric, the corresponding fabric log is deleted.	Click **Yes** to unpersist the fabric or **No** to cancel the operation.
`Fabric not persisted.`	The user attempted to refresh or clear the **Log** dialog, after a fabric was unpersisted. When you unpersist a fabric, the corresponding fabric log is deleted.	Clear the **Log** dialog after the fabric is unpersisted.

Message	Description	Action
`Field cannot be blank.`	The data field requires an entry and cannot be left blank.	Enter appropriate information in the data field.
`Field has exceeded maximum number of characters.`	The maximum number of data entry characters allowed in the field was exceeded.	Enter the information using the proscribed number of characters.
`File transfer aborted.`	The user aborted the file transfer process.	Verify the file transfer is to be aborted, then click **OK** to continue.
`HAFM error <error number 1 through 8 >.`	The *HAFM* application encountered an internal error (**1** through **8** inclusive) and cannot continue operation.	Contact the next level of support to report the problem.
`HAFM server could not log you on. Verify your username and password.`	The incorrect user name and password (both case sensitive) were used while attempting to login to the *HAFM* application.	Verify the user name and password with the customer's network administrator and retry the operation.
`HAFM server is shutting down. Connection will be terminated.`	The *HAFM* application is closing and terminating communication with the attached product.	Reboot the HAFM server. If the problem persists, contact the next level of support.
`HAFM session is already active from this workstation.`	An HAFM session already exists on the current workstation.	A workstation can have only one active HAFM session.
`Invalid character in field.`	An invalid character was entered in the data field.	Remove invalid characters from the entry.

Message	Description	Action
`Invalid name.`	One of the following invalid names was used: CON, AUX, COM1, COM2, COM3, COM4, COM5, COM6, COM7, COM8, COM9, LPT1, LPT2, LPT3, LPT4, LPT5, LPT6, LPT7, LPT8, LPT9, NUL, or PRN.	Select a valid name and retry the operation.
`Invalid network address.`	The IP address specified for the product is unknown to the domain name server (invalid).	Verify and enter a valid product IP address.
`Invalid port number. Valid ports are (0-< nn >).`	You have specified an invalid port number.	Specify a valid port number, in the range 0 to the maximum number of ports on the product minus 1. For example, for a switch with 32 ports, the valid port range is 0–31.
`Invalid product selection.`	At the **New Product** dialog box, an invalid product was selected.	Select a valid product and retry the operation.
`Invalid request.`	Three conditions result in this message: • The user tried to add or modify a product from product view and the network address is already in use. (Network addresses must be unique.) • The user tried to create a new user with a user name that already exists. (User names must be unique.) • The user tried to delete default Administrator user. (The default Administrator user cannot be deleted.)	Select the action that is appropriate to the activity that caused the error: • Network address: Specify a unique network address for the product. • User name: Specify a unique user name for the new user ID. Do not delete the default Administrator user.

Message	Description	Action
`Invalid UDP port number.`	The specified user datagram protocol (UDP) port number is invalid. The number must be an integer from **1** through **65535** inclusive.	Verify and enter a valid UDP port number.
`Invalid World-Wide Name.`	The specified world-wide name format is invalid. The valid format is eight two-digit hexadecimal numbers separated by colons (**xx:xx:xx:xx:xx:xx:xx:xx**).	Enter a world-wide name using the correct format.
`Invalid World Wide Name or nickname.`	The World Wide Name or nickname that you have specified is invalid. The valid format for the World Wide Name is eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx:xx:xx:xx:xx). The valid format for a nickname is non blank characters, up to 32 characters.	Try the operation again using a valid World Wide Name or nickname.
`Invalid zone in zone set.`	The defined zone no longer exists and is invalid.	Delete the invalid zone from the zone set.
`Limit exceeded.`	You cannot add a new product or user to HAFM if the maximum number of that resource already exists on the system.	Delete unneeded products or users from the system, before attempting to add any new ones.
`McDATA SANtegrity Feature not installed. Please contact your sales representative.`	User selected Fabric Binding or Enterprise Fabric Mode from the Fabrics menu, but the SANtegrity feature was not installed.	Install the SANtegrity feature to use Fabric Binding or enable Enterprise Fabric Mode.
`No address selected.`	You cannot complete the operation because an address has not been selected.	Select an address and retry the operation.

Message	Description	Action
`No attached nodes selected.`	An operation was attempted without an attached node selected.	Select an attached node and try the operation again.
`No HAFM server specified.`	An HAFM server is not defined to the *HAFM* application.	At the HAFM Login screen, type a server name in the **HAFM server** field and click **Login**.
`No nickname selected.`	No nickname was selected when the command was attempted.	Select a nickname and try again.
`No product managers installed.`	No director or switch *Product Manager* application is installed on this workstation.	Install the appropriate Product Manager to this workstation.
`No routing information available.`	No information is available for the route selected.	Select a different route and try the operation again.
`No user selected.`	A user was not selected when the command was attempted.	Select a user and try again.
`No zone member selected.`	A zoning operation was attempted without a zone member selected.	Select a zone member and try the operation again.
`No zone selected.`	A zoning operation was attempted without a zone selected.	Select a zone and try the operation again.
`No zone selected or zone no longer exists.`	A zoning operation was attempted without a zone selected, or the zone selected no longer exists in the fabric.	Select a zone and try the operation again.
`No zone set active.`	A zone set cannot be deactivated if there are no active zones.	Informational message only-no action is required.
`No zone set selected.`	A zoning operation was attempted without a zone set selected.	Select a zone set and try the operation again.

Message	Description	Action
`No zone set selected or zone set no longer exists.`	A zoning operation was attempted without a zone set selected, or the zone set you selected no longer exists in the fabric.	Select a zone set and try the operation again.
`Only attached nodes can be displayed in this mode.`	Users cannot display unused ports when adding ports by world-wide name.	Change the add criteria to Add by Port.
`Password and confirmation don't match.`	Entries in the password field and confirmation password field do not match. The entries are case sensitive and must be the same.	Enter the password and confirmation password again.
`Product manager instance is currently open.`	A product cannot be deleted while an instance of the *Product Manager* application is open.	Close the *Product Manager* application, then delete the product.
`Remote session support has been disabled.`	The connection between the specified remote workstation and the HAFM server was disallowed.	Consult with the customer's network administrator to determine if the workstation entry should be modified at the **Session Options** dialog box.
`Remote sessions are not allowed from this network address.`	Only IP addresses of remote workstations specified at the **Session Options** dialog box are allowed to connect to the HAFM server.	Consult with the customer's network administrator to determine if the IP address is to be configured for remote sessions.
`Resource is unavailable.`	The specified operation cannot be performed because the product is unavailable.	Verify the HAFM server-to-product link is up. If the link is up, the HAFM server may be busy. Try the operation again later.

Message	Description	Action
`Selection is not a World-Wide Name.`	The selection made is not a world-wide name.	Select a valid world-wide name before performing this operation.
`Server shutting down.`	The *HAFM* application is closing and terminating communication with the attached product.	Reboot the HAFM server. If the problem persists, contact the next level of support.
`SNMP trap address not defined.`	If an SNMP community name is defined, a corresponding SNMP trap recipient address must also be defined.	Enter a corresponding SNMP trap recipient address.
`The Administrator user cannot be deleted.`	The administrator user is permanent and cannot be deleted from the **Configure Users** dialog box.	Informational message only-no action is required.
`The Domain ID was not accepted. The World Wide Name and Domain ID must be unique in the Fabric Membership List.`	User attempted to add a detached switch to the Fabric Membership List through the Fabric Binding option (SANtegrity feature), but a switch already exists in the fabric with the same domain ID.	Enter a unique domain ID for the switch in the **Add Detached Switch** dialog box.
`The link to the director is not available.`	The Ethernet connection between the HAFM server and switch is down or unavailable.	Establish and verify the network connection.
`The maximum number of members has already been configured.`	The maximum number of unique members is 4097. The maximum number of members is 8192.	Delete members that are no longer needed to allow new members to be configured.
`The maximum number of open products has already been reached.`	The maximum number of open products allowed was reached.	Close a Product Manager session (existing open product) before opening a new session.

Message	Description	Action
The maximum number of products has already been configured.	The number of managed HP products (48) that can be defined to the *HAFM* application was reached.	Delete an existing product before adding a new product.
The maximum number of products of this type has already been configured.	The number of HP products of this type (48) that can be defined to the *HAFM* application was reached.	Delete an existing product of this type before adding a new product.
The maximum number of remote network addresses has already been configured.	A maximum of four IP addresses for remote workstations can be configured at the **Session Options** dialog box. That number was reached.	Delete an existing IP address before adding a new IP address.
The maximum number of users has already been configured.	The number of users (32) that can be defined to the *HAFM* application was reached.	Delete an existing user before adding a new user.
The maximum number of zone sets has already been configured.	The maximum number of zone sets that can be defined was reached.	Delete an existing zone set before adding a new zone set.
The maximum number of zones allowed has already been configured.	The maximum number of zones that can be defined was reached.	Delete an existing zone before adding a new zone.
The maximum number of zones per zone set has already been configured.	The maximum number of zones that can be defined in a zone set was reached.	Delete an existing zone before adding a new zone to the zone set.

Message	Description	Action
The nickname does not exist.	The entered nickname does not exist in the fabric.	Configure the nickname to the appropriate product or select an existing nickname.
The nickname is already assigned. Either use a different name or do not save the name as a nickname.	The entered nickname already exists in the fabric. Each nickname must be unique.	Define a different nickname.
The software version on this HAFM server is not compatible with the version on the remote HAFM server.	A second HAFM server PC (client) connecting to the HAFM server must be running the same software version to log in.	Upgrade the software version on the downlevel HAFM server PC.
The zoning library conversion must be completed before continuing.	The zoning library conversion is incomplete and the requested operation cannot continue.	Complete the zoning library conversion, then retry the operation.
This fabric log is no longer valid because the fabric has been unpersisted.	The selected fabric log is no longer available because the fabric has been unpersisted.	To start a new log for the fabric, persist the fabric through the **Persist Fabric** dialog box.
This network address has already been assigned.	The specified IP address was assigned and configured. A unique address must be assigned.	Consult with the customer's network administrator to determine a new IP address to be assigned and configured.

Message	Description	Action
This product is not managed by this HAFM server.	The product selected is not managed by this HAFM server.	Select a product managed by this HAFM server or go to the HAFM server that manages the affected product.
This switch is currently part of this fabric and cannot be removed from the Fabric Membership List. Isolate the switch from the fabric prior to removing it from the Fabric Membership List.	User attempted to remove a switch from the Fabric Membership List using the Fabric Binding option, but the switch is still part of the fabric.	Remove the switch from the fabric by setting the switch offline or blocking the E_Port where the switch is connected.
This user name has already been assigned.	The specified user name is already assigned and configured.	Modify (to make it unique) or delete the duplicate name.
This Worldwide Name was not accepted. The World Wide Name and Domain ID must be unique in the Fabric Membership List.	User attempted to add a detached switch to the Fabric Membership List through the Fabric Binding option (SANtegrity feature), but an entry already exists in the Fabric Membership List with the same World Wide Name (WWN).	Enter a unique World Wide Name for the switch in the **Add Detached Switch** dialog box.
Too many members defined.	The maximum number of zone members that can be defined was reached.	Delete an existing zone member before adding a new zone member.

Message	Description	Action
`You do not have rights to perform this action.`	Configured user rights do not allow this operation to be performed.	Verify user rights with the customer's network administrator and change as required.
`You must define an SMTP server address.`	A simple mail transfer protocol (SMTP) server address must be defined and configured for e-mail to be activated.	Define the SMTP server address at the **Configure E-Mail** dialog box.
`You must define at least one E-mail address.`	At least one e-mail address must be defined and configured for e-mail to be activated.	Define an e-mail address at the **Configure E-Mail** dialog box.
`You must define at least one remote network address.`	At least one IP address for a remote workstation must be configured for a remote session to be activated.	Define an IP address for at least one remote workstation at the **Session Options** dialog box.
`You must download the HAFM client via the web install.`	An attempt was made to download the *HAFM* application to a remote workstation (client) using an improper procedure.	Download a compatible version of the *HAFM* application to the remote workstation (client) using the web install procedure.
`Zones configured with port numbers are ignored in Open Fabric Mode.`	While in Open Fabric mode, zones configured using port numbers are enforced through world-wide names.	Informational message only — no action is required.
`Zones must be defined before creating a zone set.`	You cannot create a zone set without any zones defined for HAFM.	Define zones using the **New Zone** dialog box.
`Zoning by port number is ignored in Open Fabric Mode.`	While in Open Fabric mode, zones configured using port numbers are enforced through world-wide names.	Informational message only — no action is required.

Message	Description	Action
`Zoning by port number is not supported in Open Fabric Mode.`	You cannot specify an item for zoning by port number if HAFM is in Open Fabric Mode.	Define zones by WWN of device.
`Zoning name already exists.`	Duplicate zone names are not allowed in the zoning library.	Modify (to make it unique) or delete the duplicate zone name.

Edge-32 Switch Product Manager Messages

This section lists switch Product Manager information and error messages in alphabetical order.

Message	Description	Action
`All port names must be unique.`	A duplicate Fibre Channel port name was configured. All port names must be unique.	Reconfigure the Fibre Channel port with a unique name.
`Another product manager is currently performing a firmware install.`	Only one instance of the *Product Manager* application can install a firmware version to the switch or director at a time.	Wait for the firmware installation process to complete and try the operation again.
`Are you sure you want to delete firmware version?`	This message requests confirmation to delete a firmware version from the HAFM server's firmware library.	Click **Yes** to delete the firmware version or **No** to abort the operation.
`Are you sure you want to send firmware version?`	This message requests confirmation to send a firmware version from the HAFM server's firmware library to the switch or director.	Click **Yes** to send the firmware version or **No** to abort the operation.

Message	Description	Action
Cannot change Port Type while in S/390 mode without SANtegrity feature. Please contact your sales representative.	User attempted to change a port type in the **Configure Ports** dialog box while in S/390 mode, but the optional SANtegrity feature is not installed.	Informational message. Install SANtegrity before changing port types in the **Configure Ports** dialog box while in S/390 operating mode.
Cannot disable Switch Binding while Enterprise Fabric Mode is active and the switch is Online.	User attempted to disable switch binding through the **Switch Binding Change State** dialog box, but Enterprise Fabric Mode is enabled.	You must either disable Enterprise Fabric Mode using the **Enterprise Fabric Mode** dialog box in the *HAFM* application or set the switch offline before you can disable Switch Binding.
Cannot disable Insistent Domain ID while Fabric Binding is active	User attempted to disable the Insistent Domain ID parameter through the **Configure Switch Parameters** dialog box, but Fabric Binding is enabled.	Disable Fabric Binding through the **Fabric Binding** dialog box before disabling these parameters.
Cannot enable beaconing on a failed FRU.	Occurs when selecting Enable Beaconing option for a failed FRU.	Replace FRU and enable beaconing again or enable beaconing on operating FRU.
Cannot enable beaconing while the system error light is on.	Beaconing cannot be enabled while the system error light is on.	Select **Clear System Error Light** from the **Product** menu to clear error light, then enable beaconing.

Message	Description	Action
`Cannot have E-Ports configured in S/390 mode Unless SANtegrity feature is installed. Please contact your sales representative.`	User attempted to change operating mode from Open Systems to S/390 mode with E_Ports configured but SANtegrity is not installed.	Informational message. If you install SANtegrity before changing to S/390 mode, then E_Ports will remain as E_Ports when you change to S/390 mode. If SANtegrity is not installed, setting a switch to S/390 mode will change all E_Ports to G_Ports.
`Cannot have spaces in field.`	Spaces are not allowed as part of the entry for this field.	Delete spaces from the field entry.
`Cannot perform this operation while the switch is offline.`	This operation cannot take place while the switch is offline.	Configure the switch offline through the **Set Online State** dialog box then retry the operation.
`Cannot retrieve current SNMP configuration.`	The current SNMP configuration cannot be retrieved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
`Cannot retrieve diagnostics results.`	Switch or director diagnostic results cannot be retrieved by the *Product Manager* application because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
`Cannot retrieve director date and time.`	The switch or director date and time cannot be retrieved by the *Product Manager* application because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.

Message	Description	Action
Cannot retrieve director state.	The switch or director state cannot be retrieved by the *Product Manager* application because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot retrieve information for port.	Information for the port cannot be retrieved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot retrieve port configuration.	The port configuration cannot be retrieved by the *Product Manager* application because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot retrieve port information.	Port information cannot be retrieved by the *Product Manager* application because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot retrieve port statistics.	Port statistics cannot be retrieved by the *Product Manager* application because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot run diagnostics on a port that is failed.	Port diagnostics cannot be performed on a port that has failed.	Run diagnostics only on an operational port.
Cannot run diagnostics on a port that is not installed.	Port diagnostics (loopback tests) cannot be performed on a port that does not have a small form factor pluggable (SFP) optical transceiver installed.	Install a transceiver in the port and perform diagnostics again.
Cannot run diagnostics while a device is logged-in to the port.	Port diagnostics (internal loopback test) cannot be performed on a port while an attached Fibre Channel device is logged in.	Ensure the device is logged out and perform diagnostics again.

Message	Description	Action
Cannot save port configuration.	The port configuration cannot be saved at the *Product Manager* application because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot save SNMP configuration.	The switch or director SNMP configuration cannot be saved at the *Product Manager* application because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot set all ports to 1 Gb/sec due to port speed restriction on some ports.	Displays if you try to set ports to operate at 1 Gb/sec data speed through the **Configure Ports** dialog box and some ports do not support speed configuration.	Replace ports that do not support speed configuration with those that do support more than one speed configuration.
Cannot set all ports to 2Gb/sec due to port speed restriction on some ports.	Displays if you try to set ports to operate at 2 Gb/sec data speed through the **Configure Ports** dialog box and some ports do not support speed configuration.	Replace ports that do not support speed configuration with those that do support more than one speed configuration.
Cannot set all ports to Negotiate due to port speed restriction on some ports.	Displays if you try to set all ports to **Negotiate** through the **Configure Ports** dialog box and some ports do not support speed configuration.	Replace ports that do not support speed configuration with those that do support more than one speed configuration.
Cannot set director date and time.	The switch or director date and time cannot be set at the *Product Manager* application because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot set director state.	The switch or director state cannot be set at the *Product Manager* application because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.

Message	Description	Action
Cannot set fibre channel parameters.	Fibre Channel parameters for the switch or director cannot be set at the *Product Manager* application because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot start data collection.	The data collection procedure cannot be started by the *Product Manager* application because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Cannot start port diagnostics.	Port diagnostics cannot be started at the *Product Manager* application because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Click OK to remove all contents from log.	This action deletes all contents from the selected log.	Click **OK** to delete the log contents or Cancel to cancel the operation.
Connection to HAFM Server lost.	The connection to the remote HAFM server has been lost.	Log in to the HAFM server again through the **HAFM Manager Login** dialog box.
Connection to HAFM server lost. Click OK to exit application.	The *HAFM* application at a remote workstation lost the network connection to the HAFM server.	Start the *HAFM* application to connect to the HAFM server.
Could not export log to file.	A log file I/O error occurred and the file could not be saved to the specified destination. The disk may be full or write protected.	If the disk is full, use another disk. If the disk is write protected, change the write-protect properties or use another disk.

Message	Description	Action
`Could not find firmware file.`	A firmware version could not be found because the data directory structure for the HAFM server is corrupt.	Reinstall the *HAFM* and *Product Manager* applications. If the condition persists, contact the next level of support.
`Could not remove dump files from server.`	Dump files could not be deleted from the HAFM server because the notebook PC or *Product Manager* application is busy.	Retry the operation later. If the condition persists, contact the next level of support.
`Could not stop port diagnostics.`	Port diagnostics could not be stopped by the *Product Manager* application because the Ethernet link is down or busy, or because the switch or director is busy.	Retry the operation later. If the condition persists, contact the next level of support.
`Could not write firmware to flash.`	A firmware version could not be written from the HAFM server to FLASH memory on the switch's CTP2 card.	Retry the operation again. If the condition persists, contact the next level of support.
`Date entered is invalid.`	The date is entered incorrectly at the **Configure Date and Time** dialog box. Individual field entries may be correct, but the overall date is invalid (for example, a day entry of **31** for a 30-day month).	Verify each entry is valid and consistent.

Message	Description	Action
[device WWN] cannot be removed from the Switch Membership List while participating in Switch Binding. The device must be isolated from the switch, or Switch Binding deactivated before it can be removed.	User attempted to remove a device WWN from the Switch Membership List (SANtegrity feature) while Switch Binding is enabled.	Remove the device from the switch by blocking the port, setting the switch offline, or disabling Switch Binding through the **Switch Binding Change State** dialog box before removing devices from the Switch Membership List.
Device applications should be terminated before starting diagnostics. Press NEXT to continue.	Port diagnostics (loopback tests) cannot be performed on a port while an attached device application is running.	Terminate the device application and perform diagnostics again.
Disabling Insistent Domain ID will disable Fabric Binding. Do you want to continue?	Fabric Binding is enabled through HAFM and user attempted to disable Insistent Domain ID in the **Configure Switch Parameters** dialog box.	Click **Yes** if you want to continue and disable Fabric Binding.
Disabling Switch Binding will disable Enterprise Fabric Mode. Do you want to continue?	User attempted to disable Switch Binding through the **Switch Binding State Change** dialog box, but Enterprise Fabric Mode is enabled.	Disable Enterprise Fabric Mode through the **Enterprise Fabric Mode** dialog box before disabling Switch Binding.

Message	Description	Action
Do you want to continue with IPL?	This message requests confirmation to initial program load (IPL) the switch or director.	Click **OK** to IPL the switch or director or **No** to cancel the operation.
Duplicate Community names require identical write authorizations.	Duplicate community names are entered at the **Configure SNMP** dialog box, and have different write authorizations.	Delete the duplicate community name or make the write authorizations consistent.
Enterprise Fabric Mode will be disabled if any of the following parameters are disabled: Insistent Domain ID, Rerouting Delay, Domain RSCNs. Do you want to continue?	User attempted to disable these parameters in the **Configure Switch Parameters** dialog box while the switch was online, but Enterprise Fabric Mode (SANtegrity feature) is enabled.	Click **Yes** if you want to continue, and disable Enterprise Fabric Mode.
Error retrieving port information.	An error occurred at the *Product Manager* application while retrieving port information because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Error retrieving port statistics.	An error occurred at the *Product Manager* application while retrieving port statistics because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.
Error stopping port diagnostics.	An error occurred at the *Product Manager* application while attempting to stop port diagnostics from running because the Ethernet link is down or busy.	Retry the operation later. If the condition persists, contact the next level of support.

Message	Description	Action
`Error transferring files < message >.`	An error occurred while transferring files from the PC hard drive to the *Product Manager* application. The message varies, depending on the problem.	Try the file transfer operation again. If the problem persists, contact the next level of support.
`Field cannot be blank.`	The data field requires an entry and cannot be left blank.	Enter appropriate information in the data field.
`File transfer aborted.`	The user aborted the file transfer process.	Verify the file transfer is to be aborted, then click **OK** to continue.
`File transfer is in progress.`	A firmware file is being transferred from the HAFM server hard drive, or a data collection file is being transferred to a diskette.	Informational message only-no action is required.
`Firmware download timed out.`	The switch did not respond in the time allowed. The status of the firmware install operation is unknown.	Retry the operation. If the problem persists, contact support personnel.
`Firmware file I/O error.`	A firmware download operation aborted because a file I/O error occurred.	Retry the operation. If the problem persists, contact the next level of support.
`Firmware file not found.`	The firmware version is not installed (or was deleted) from the firmware library at the HAFM server.	Add the firmware version to the library and retry the operation.
`Incorrect product type.`	When configuring a new product through the **New Product** dialog box, an incorrect product was selected for the network address.	Select the correct product type for the product with the network address.

Message	Description	Action
Installing this feature key, while online, will cause an IPL operation on the switch and a momentary loss of LAN connection. This operation is non-disruptive to the Fibre Channel traffic. Do you wish to continue installing this feature key?	If the switch is online, installing the new feature key will cause an internal program load (IPL). The LAN connection to the HAFM server will be lost momentarily, but Fibre Channel traffic will not be affected.	Select **Yes** to install the feature key or **No** to not install.
Internal file transfer error received from director.	The switch or director detected an internal file transfer error.	Retry the operation. If the problem persists, contact the next level of support.
Invalid character in field.	An invalid character was entered in the data field.	Remove invalid characters from the entry.
Invalid configuration name.	Attempted to save an address configuration name with an invalid name.	Use up to 24 alphanumeric characters, including spaces, hyphens and underscores.
Invalid firmware file.	The file selected for firmware download is not a firmware version file.	Select the correct firmware version file and retry the operation.
Invalid network address.	The IP address specified for the product is unknown to the domain name server (invalid).	Verify and enter a valid product IP address.

Message	Description	Action
`Invalid port number.`	The Fibre Channel number entered is invalid. The port number must be an integer from **0** through **63** inclusive.	Verify and enter a valid port number.
`Invalid port number. Valid ports are (0 - 31).`	Port number must be within the range of ports for the specific switch model. For this model, the valid port numbers are 0 - 31.	Enter a port number within the correct range.
`Invalid response received from director.`	An error occurred at the switch or director during a firmware download operation.	Retry the firmware download operation. If the problem persists, contact the next level of support.
`Invalid UDP port number.`	The specified user datagram protocol (UDP) port number is invalid. The number must be an integer from **1** through **65535** inclusive.	Verify and enter a valid UDP port number.
`Invalid value for BB_Credit.`	At the **Configure Operating Parameters** dialog box, the buffer-to-buffer credit (BB_Credit) value must be an integer from **1** through **60** inclusive.	Verify and enter a valid number.
`Invalid value for day (1 - 31).`	At the **Configure Date and Time** dialog box, the *DD* value (day) must be an integer from **1** through **31** inclusive.	Verify and enter a valid date.
`Invalid value for E_D_TOV.`	At the **Configure Operating Parameters** dialog box, the error detect time-out value (*E_D_TOV*) must be an integer from **2** through **600** inclusive.	Verify and enter a valid number.
`Invalid value for hour (0 - 23).`	At the **Configure Date and Time** dialog box, the HH value (hour) must be an integer from **0** through **23** inclusive.	Verify and enter a valid time.

Message	Description	Action
`Invalid value for minute (0 - 59).`	At the **Configure Date and Time** dialog box, the MM value (minute) must be an integer from **0** through **59** inclusive.	Verify and enter a valid time.
`Invalid value for month (1 - 12).`	At the **Configure Date and Time** dialog box, the MM value (month) must be an integer from **1** through **12** inclusive.	Verify and enter a valid date.
`Invalid value for R_A_TOV.`	At the **Configure Operating Parameters** dialog box, the resource allocation time-out value (*R_A_TOV*) must be an integer from **10** through **1200** inclusive.	Verify and enter a valid number.
`Invalid value for second (0 - 59).`	At the **Configure Date and Time** dialog box, the SS value (second) must be an integer from **0** through **59** inclusive.	Verify and enter a valid time.
`Invalid value for year.`	At the **Configure Date and Time** dialog box, the YYYY value (year) must be a four-digit value.	Verify and enter a four-digit value for the year.
`Invalid World-Wide Name.`	The specified world-wide name format is invalid. The valid format is eight two-digit hexadecimal numbers separated by colons (`xx:xx:xx:xx:xx:xx:xx:xx`).	Enter a world-wide name using the correct format.
`Invalid World Wide Name or nickname.`	The World Wide Name or nickname that you have specified is invalid. The valid format for the World Wide Name is eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx:xx:xx:xx:xx). The valid format for a nickname is non blank characters, up to 32 characters.	Try the operation again using a valid World Wide Name or nickname.

Message	Description	Action
Link dropped.	The HAFM server-to-switch or director Ethernet link was dropped.	Retry the operation. If the condition persists, contact the next level of support.
Log is currently in use.	Access to the log is denied because the log was opened by another instance of the *Product Manager* application.	Retry the operation later. If the condition persists, contact the next level of support.
Maximum number of versions already installed.	The number of firmware versions that can be defined to the *HAFM* application's firmware library was reached.	Delete an existing firmware version before adding a new version.
McDATA SANtegrity Feature not installed. Please contact your sales representative.	The user selected Switch Binding from the **Configure** menu, but the optional SANtegrity feature is not installed.	Install the SANtegrity key through the **Configure Feature Key** dialog box before using Switch Binding features.
No file was selected.	Action requires the selection of a file.	Select a file.
No firmware versions to delete.	There are no firmware versions in the firmware library to delete, therefore the operation cannot be performed.	Informational message only-no action is required.
No firmware version was selected.	A file was not selected in the **Firmware Library** dialog box before an action, such as modify or send, was performed.	Click a firmware version in the dialog box to select it, then perform the action again.
Non-redundant switch must be offline to install firmware.	Since the switch has only a single CTP card, it must be offline to initiate a firmware installation.	Take switch offline and try again.

Message	Description	Action
`Not all of the optical transceivers are installed for this range of ports.`	Some ports in the specified range do not have optical transceivers installed.	Use a port range that is valid for the ports installed.
`Performing this action will overwrite the date/time on the director.`	Warning that occurs when configuring the date and time through the **Configure Date and Time** dialog box, that the new time or date will overwrite the existing time or date set for the switch or director.	Verify that you want to overwrite the current date or time.
`Performing this operation will change the current state to Offline.`	This message requests confirmation to set the switch or director offline.	Click **OK** to set the switch or director offline or **Cancel** to cancel the operation.
`Performing this operation will change the current state to Online.`	This message requests confirmation to set the switch or director online.	Click **OK** to set the switch or director online or **Cancel** to cancel the operation.
`Periodic Date/Time synchronization must be cleared.`	Action cannot be performed because Periodic Date/Time Synchronization option is active.	Click **Periodic Date/Time Synchronization** check box in **Configure Date and Time** dialog box (**Configure** menu) to clear check mark and disable periodic date/time synchronization.

Message	Description	Action
Port binding was removed from attached devices that are also participating in Switch Binding.	Informational message. User has removed Port Binding from attached devices, but one or more of these devices is still controlled by Fabric Binding.	Review the Switch Binding Membership List to determine if the devices should be members.
Port diagnostics cannot be performed on an inactive port.	This displays when port diagnostics is run on a port in an inactive state.	Run the diagnostics on an active port.
Port speeds cannot be configured at a higher rate than the director/switch speed.	This displays when you configure a port to 2 GB/sec and the switch speed is set to 1 Gb/sec.	Set the port speed to 1 Gb/sec in the **Configure Ports** dialog box.
Product manager error < error number 5001 or 5002 >.	At the **Configure Operating Parameters** dialog box, the *R_A_TOV* entry must be greater than *E_D_TOV* entry.	Verify and change one of the entries to make the relationship valid.
Product manager instance is currently open.	A Product Manager window is open.	Informational message only.
Resource is unavailable.	The specified operation cannot be performed because the product is unavailable.	Verify that the HAFM server-to-product link is up. If the link is up, the HAFM server may be busy. Try the operation again later.
Send firmware failed.	A firmware download operation failed.	Retry the firmware download operation. If the problem persists, contact the next level of support.

Message	Description	Action
SNMP trap address not defined.	If an SNMP community name is defined, a corresponding SNMP trap recipient address must also be defined.	Enter a corresponding SNMP trap recipient address.
Stop diagnostics failed. The test is already running.	Diagnostics for the port was not running and the Stop was selected on the **Port Diagnostics** dialog box. Diagnostics quit for the port, but **Stop** button remains enabled.	Verify port operation. Retry diagnostics for port and select **Stop** from the dialog box. If problem persists, contact your service representative.
Stop diagnostics failed. The test was not running.	The action to stop diagnostics failed because the test was not running.	Informational message.
Switch Binding was removed from attached devices that are also participating in Port Binding. Please review the Port Binding Configuration.	The device WWNs were removed from the director's Switch Membership List (SANtegrity Switch Binding feature), but you should note that one or more of these devices still has security control in port binding.	Verify that the security level for each device is as required by reviewing the Bound WWN list in the **Configure Ports** dialog box.
System diagnostics cannot run. The Operational Status is invalid.	System diagnostics cannot run on switch or directors or switches with failed ports.	Replace failed ports.
The add firmware process has been aborted.	The user aborted the process to add a firmware version to the HAFM server's firmware library.	Verify the firmware addition is to be aborted, then click **OK** to continue.
The data collection process failed.	An error occurred while performing the data collection procedure.	Try the data collection procedure again. If the problem persists, contact the next level of support.

Message	Description	Action
The data collection process has been aborted.	The user aborted the data collection procedure.	Verify the data collection procedure is to be aborted, then click **OK** to continue.
The default zone must be disabled to configure.	The message displays when the user attempts to change the operating mode to the open fabric mode and the default zone is enabled.	Disable the default zone and repeat the operation.
The firmware file is corrupted.	A firmware version file is corrupt.	Contact the next level of support to report the problem.
The firmware version already exists.	This firmware version already exists in HAFM server's firmware library.	Informational message only-no action is required.
The following parameters cannot be disabled while Enterprise Fabric Mode is active: Insistent Domain ID, Rerouting Delay, Domain RSCNs.	User attempted to disable these parameters in the **Configure Switch Parameters** dialog box while Enterprise Fabric Mode is enabled.	Disable Enterprise Fabric Mode through the **Enterprise Fabric Mode** dialog box in HAFM, then disable the parameters.
The HAFM server is busy processing a request from another product manager.	The HAFM server PC is processing a request from another instance of a *Product Manager* application, and cannot perform the requested operation.	Wait until the process is completes, then perform the operation again.
The IPL configuration cannot be deleted.	Deletion of the IPL address configuration was attempted and was not allowed.	Cancel the operation.

Message	Description	Action
The link to the director is not available.	The Ethernet connection between the HAFM server and the switch or director is down or unavailable.	Establish and verify the network connection.
This feature has not been installed. Please contact your sales representative.	Indicator that the feature has not been installed on this switch.	Contact your sales representative to obtain the desired feature.
This feature key does not include all of the features currently installed and cannot be activated while the switch is online.	The feature set currently installed for this system contains features that are not being installed with the new feature key. To activate the new feature key, you must set the switch offline. Activating the new feature set, however, will remove current features not in the new feature set.	Set the switch offline through the **Set Online State** dialog box, then activate the new feature key using the **Configure Feature Key** dialog box.
Threshold alerts are not supported.	Threshold alerts are not supported in firmware releases before 1.03.00.	Informational message.
Unable to change to incompatible firmware release.	The user tried to download a firmware release that is not compatible with the current product configuration.	Refer to the release notes or contact customer support.
Unable to save data collection file to destination.	The HAFM server could not save the data collection file to the specified location (PC hard drive, diskette, or network).	Retry the operation. If the condition persists, contact the next level of support.
You do not have rights to perform this action.	Configured user rights do not allow this operation to be performed.	Verify user rights with the customer's network administrator and change as required.

B

Event Codes

This appendix lists all three-digit HP StorageWorks Edge Switch 2/32 event codes and provides detailed information about each code. Event codes are listed in numerical order and in tabular format.

An event is an occurrence (state change, problem detection, or problem correction) that requires user attention or that should be reported to a system administrator or service representative. An event usually indicates a switch operational state transition, but may also indicate an impending state change (threshold violation). An event may also provide information only, and not indicate an operational state change. Event codes are grouped as follows:

- **000** through **199 —** system events.
- **200** through **299 —** power supply events.
- **300** through **399 —** fan module events.
- **400** through **499 —** CTP card events.
- **500** through **599 —** port module events.
- **600** through **699 —** SBAR events.
- **700** through **799 —** Reserved for future use.
- **800** through **899 —** Thermal

Events can be recorded in the switch Event Logs at the HAFM server, or at a remote workstation if E-mail and call-home features are enabled. An event may also illuminate the system error (**ERR**) light-emitting diode (LED) on the front panel.

In addition to numerical event codes, the tables in this appendix also provide a:

- **Message —** a brief text string that describes the event.
- **Severity —** a severity level that indicates event criticality as follows:
  - **0 —** informational.
  - **2 —** minor.

— **3 —** major.

— **4 —** severe (not operational).

- **Explanation —** a complete explanation of what caused the event.
- **Action —** the recommended course of action (if any) to resolve the problem.
- **Event Data —** supplementary event data (if any) that displays in the event log in hexadecimal format.
- **Distribution —** check marks in associated fields indicate where the event code is reported (front panel, HAFM server, or host).

System Events (000 through 199)

Event Code: 001							
Message:	`System power-down.`						
Severity:	Informational.						
Explanation:	The switch was powered off or disconnected from the facility AC power source. The event code is distributed the next time the switch powers on, but the date and time of the code reflect the power-off time.						
Action:	No action required.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 011	
Message:	`Login Server database invalid.`
Severity:	Minor.
Explanation:	Following an initial machine load (IML) or firmware download, the Login server database failed its cyclic redundancy check (CRC) validation. All Fabric Services databases are initialized to an empty state, resulting in an implicit Fabric logout of all attached devices.
Action:	Perform the data collection procedure and return the Zip disk to HP support personnel.
Event Data:	No supplementary data included with this event.

Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔		

Event Code: 021							
Message:	`Name Server database invalid.`						
Severity:	Minor.						
Explanation:	Following an IML or firmware download, the Name server database failed its CRC validation. All Fabric Services databases are initialized to an empty, state resulting in an implicit Fabric logout of all attached devices.						
Action:	Perform the data collection procedure and return the Zip disk to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔		

Event Code: 031							
Message:	`SNMP request received from unauthorized community.`						
Severity:	Informational.						
Explanation:	An SNMP request containing an unauthorized community name was received and rejected with an error. Only requests containing authorized SNMP community names as configured through the switch *Product Manager* application are allowed.						
Action:	Add the community name to the SNMP configuration using the switch *Product Manager* application.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 051							
Message:	Management Server database invalid.						
Severity:	Minor.						
Explanation:	Following an IML, or firmware download, the Management server database failed its CRC validation. All Management Services databases are initialized to an empty state, resulting in an implicit logout of all devices logged in to the Management server.						
Action:	Perform the data collection procedure and return the Zip disk to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔		

Event Code: 052	
Message:	Management Server internal error, an indication of asynchronous status report activation, or an indication that a mode register update has occurred.
Severity:	Informational.
Explanation:	The Management server subsystem detected an internal operating error within the switch, or an asynchronous status is to be reported to a Host, or an indication that a mode register has occurred.
Action:	For a management server internal error, perform the data collection procedure for the switch using HAFM, save the data file to the HAFM server Zip drive, and return the Zip disk to HP Services for analysis. If the event is a synchronous status report or a mode register update no action is required.
Event Data:	The data reported consists of an indication that the reporting tasks are of type **eMST_SB2**, the component_id is **eMSCID_SB2_CHPGM**. In the event of an actual error the subcomponent_id is **eMS_ELR_SB2_DEVICE_PROTOCOL_ERROR** or **eMS_ELR_SB2_MSG_PROCESSING_ERROR**. When asynchronous status is to be reported the subcomponent_id is **eSB2_CP_RER_ASYNCH_STATUS_REPORTING**. In the event of a Mode Register update, the subcomponent_id is **eMS_ELR_MODE_REGISTER_UPDATE**. Any other data elements are used by the developers to evaluate errors.

Distribution:	Switch		HAFM Server			Host	
	Nonvola-tile System Event Log	System Error Indicator	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔		✔			✔	

Event Code: 061							
Message:	`Fabric Controller database invalid.`						
Severity:	Minor.						
Explanation:	Following an IML, or firmware download, the Fabric Controller database failed its CRC validation. All Fabric Controller databases are initialized to an empty state, resulting in a momentary loss of interswitch communication capability.						
Action:	Perform the data collection procedure and return the Zip disk to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔		

Event Code: 062	
Message:	`Maximum interswitch hop count exceeded.`
Severity:	Informational.
Explanation:	The Fabric Controller software has detected that a path to another switch in the fabric traverses more than seven interswitch links (hops). This may result in frames persisting in the fabric longer than the Fibre Channel standard time-out values allow.
Action:	If possible, reconfigure the fabric so that the path between any two switches traverses no more than seven interswitch links.
Event Data:	Byte **0** = domain ID of the switch more than seven hops away. Bytes **1–3** = Reserved.

Distribution:	Switch		HAFM Server			Host	
	Nonvolatile System Event Log	System Error Indicator	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔		✔				

Event Code: 063							
Message:	`Remote switch has too many ISLs.`						
Severity:	Major.						
Explanation:	The switch indicated in the event data (Domain ID) has too many ISLs attached to it. That switch is unreachable from this switch.						
Action:	Reduce the number of ISLs on the indicated switch to a number that within the limits (128 ISLs per switch).						
Event Data:	Byte **0** = domain ID of the switch with too many ISLs. Bytes **1–3** = Reserved.						
Distribution:	Switch		HAFM Server			Host	
	Nonvolatile System Event Log	System Error Indicator	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔	✔	✔	✔			

Event Code: 070	
Message:	`E_Port is segmented.`
Severity:	Informational.
Explanation:	A switch E_Port recognized an incompatibility with an attached fabric element (director or switch), preventing the switch from participating in the fabric. A segmented port does not transmit Class 2 or Class 3 traffic (data from attached devices), but transmits Class F traffic (management and control data from the attached director or switch). Refer to the event data for the segmentation reason.
Action:	Action depends on the segmentation reason specified in the event data.

<table>
<tr><td>Event Data:</td><td colspan="7">The first byte of event data (byte 0) specifies the E_Port number. The fifth byte (byte 4) specifies the segmentation reason as follows:
1 = Incompatible operating parameters. Ether the resource allocation time out value (R_A_TOV) or error detect time out value (E_D_TOV) is inconsistent between the switch and another fabric element (director or switch). Modify the R_A_TOV and E_D_TOV to make the values consistent for all fabric directors and switches.
2 = Duplicate domain ID. The switch has the same preferred domain ID as another fabric element (director or switch). Modify the switch's Domain ID to make it unique.
3 = Incompatible zoning configurations. The same name is applied to a zone for the switch and another fabric element (director or switch), but the zones contain different zone members. Modify the zone name to make it unique, or ensure zones with the same name contain identical zone members.
4 = Build fabric protocol error. A protocol error was detected during incorporation of the switch into the fabric. Disconnect the E_Port link, reconnect the link, and initial program load (IPL) the switch. If the condition persists, perform the data collection procedure and return the Zip disk to HP support personnel.
5 = No principal switch. No director or switch in the fabric can become the principal switch. Modify the switch priority to any value other than 255.
6 = No response from attached switch (hello timeout). The switch periodically verifies operation of attached fabric elements (directors or switches). The switch E_Port (at the operational switch) times out and segments if the attached device does not respond. Check the status of the attached director or switch. If the condition persists, perform the data collection procedure (at the attached device) and return the Zip disk to HP support personnel.
7 = ELP retransmission failure timeout. A switch that exhibits a hardware or link failure attempted to join a fabric and transmitted multiple exchange link protocol (ELP) frames to a fabric element (director or switch). However, because of the problem, the switch did not receive responses to the ELP frames, and did not receive a fabric login (FLOGI) frame. After five ELP transmission attempts, the switch E_Port (failed switch) times out and segments. Refer to MAP 0000: Start MAP to perform hardware fault isolation at the failed switch.</td></tr>
<tr><td rowspan="3">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Server</td><td colspan="2">Host</td></tr>
<tr><td>EWS Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td>✔</td><td></td><td>✔</td><td></td><td></td><td></td><td></td></tr>
</table>

Event Code: 071	
Message:	`Switch is isolated.`
Severity:	Informational.

<table>
<tr><td>Explanation:</td><td colspan="7">The switch is isolated from other fabric elements (directors or switches). This event code is accompanied by one or more 070 event codes. Refer to the event data for the segmentation reason.</td></tr>
<tr><td>Action:</td><td colspan="7">Action depends on the segmentation reason specified in the event data.</td></tr>
<tr><td>Event Data:</td><td colspan="7">The first byte of event data (byte 0) specifies the E_Port number. The fifth byte (byte 4) specifies the segmentation reason as follows:
1 = Incompatible operating parameters. Ether the resource allocation time out value (R_A_TOV) or error detect time out value (E_D_TOV) is inconsistent between the switch and another fabric element (director or switch). Modify the R_A_TOV and E_D_TOV to make the values consistent for all fabric directors and switches.
2 = Duplicate domain ID. The switch has the same preferred domain ID as another fabric element (director or switch). Modify the switch's Domain ID to make it unique.
3 = Incompatible zoning configurations. The same name is applied to a zone for the switch and another fabric element (director or switch), but the zones contain different zone members. Modify the zone name to make it unique, or ensure zones with the same name contain identical zone members.
4 = Build fabric protocol error. A protocol error was detected during incorporation of the switch into the fabric. Disconnect the E_Port link, reconnect the link, and IPL the switch. If the condition persists, perform the data collection procedure and return the Zip disk to HP support personnel.
5 = No principal switch. No director or switch in the fabric can become the principal switch. Modify the switch priority to any value other than 255.
6 = No response from attached switch (hello timeout). The switch periodically verifies operation of attached fabric elements (directors or switches). The switch E_Port (at the operational switch) times out and segments if the attached device does not respond. Check the status of the attached director or switch. If the condition persists, perform the data collection procedure (at the attached device) and return the Zip disk to HP support personnel.
7 = ELP retransmission failure timeout. A switch that exhibits a hardware or link failure attempted to join a fabric and transmitted multiple ELP frames to a fabric element (director or switch). However, because of the problem, the switch did not receive responses to the ELP frames, and did not receive an FLOGI frame. After five ELP transmission attempts, the switch E_Port (failed switch) times out and segments. Refer to MAP 0000: Start MAP to perform hardware fault isolation at the failed switch.</td></tr>
<tr><td rowspan="3">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Server</td><td colspan="2">Host</td></tr>
<tr><td>EWS Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td>✔</td><td></td><td>✔</td><td></td><td></td><td></td><td></td></tr>
</table>

Event Code: 072							
Message:	E_Port connected to unsupported switch.						
Severity:	Informational.						
Explanation:	The switch is attached (through an ISL) to an incompatible fabric element (director or switch).						
Action:	Disconnect the ISL.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 073	
Message:	Fabric Init Error.
Severity:	Informational.
Explanation:	There was an error detected in the fabric initialization sequence. Most problems are caused by frame delivery errors. The Event data is intended for engineering evaluation of the problem. It includes a reason code, and if applicable, a list of ports that problems were detected over.
Action:	Perform a data collection operation and contact a service representative.
Event Data:	Byte **0**: The error Reason Code: 01 = Error no notification for principal switch. Not principal switch, and never receives AAI (DIA) from the principal switch. 02 = Error domain ID not assigned. Not principal switch and got no response to RDI. Unable to allocate a domain ID. 03 = Fabric initialization completed, and discovered neighbor switches not in local domain ID list. After the fabric init sequence completes, directly connected switches are not included in the local domain id list. 04–FF = Reserved.

Distribution:	Switch		HAFM Server			Host	
	Nonvolatile System Event Log	System Error Indicator	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔		✔				

Event Code: 074							
Message:	`ISL frame delivery error threshold.`						
Severity:	Informational.						
Explanation:	The number of fabric controller frame delivery errors exceeded a threshold over an E_Port, and fabric init problems (event 73) were detected. Most fabric init problems are due to control frame delivery problems. This event provides an indication of undelivered frames after they have caused problems with the fabric initialization process.						
Action:	Perform a data collection operation and contact a service representative.						
Event Data:	Byte **0** = E_Port port number. Byte **1–3** = Reserved Byte **4–7 =** Count of frame delivery time-out indications. Byte **8–11** = Count of frame delivery abort indications.						
Distribution:	Switch		HAFM Server			Host	
	Nonvolatile System Event Log	System Error Indicator	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔		✔				

Event Code: 080	
Message:	`Unauthorized world wide name.`
Severity:	Informational.
Explanation:	The world wide name of the switch connected to the indicated port is not authorized for that port.
Action:	Either change the port binding definition, or connect the correct switch to this port.

Event Data:	Byte **0** = failing port number. Bytes **1–3** = Reserved. Bytes **4–11** = World wide name of the unauthorized device.						
Distribution:	Switch		HAFM Server			Host	
	Nonvola-tile System Event Log	System Error Indicator	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔		✔	✔		✔	

Event Code: 081	
Message:	`Port has been set to Invalid Attachment state.`
Severity:	Informational.
Explanation:	The port has recognized an incompatibility with the device connected to the other end of the link, preventing the two devices from joining. Ports that are isolated will not carry Class 2 or Class 3 traffic, and will reject Class F traffic.
Action:	Action depends on the event data.

<table>
<tr><td>Event Data:</td><td colspan="7">Byte 0 = Port number.
Bytes 1–3 = Reserved.
Byte 4 = Reason Code:
01 = Unknown reason.
02 = Non-E_Port mode.
03 = Process ELP reject with unable to process reason code.
04 = Process ELP reject with invalid revision level.
05 = Loopback indication.
06 = Non-F_Port mode.
07 = When in legacy mode detect connection over E_Port of a non-HP switch based on the WWN.
08 = Not used.
09 = Not used.
0A = Unauthorized port binding WWN.
0B = G_Port ELP time-out.
0C = ESA security mismatch.
0D = Fabric binding mismatch.
0E = Authorization failure reject.
0F = Unauthorized switch binding.
Bytes 8–16 = WWN of device attached.</td></tr>
<tr><td rowspan="3">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Server</td><td colspan="2">Host</td></tr>
<tr><td>Nonvola-tile System Event Log</td><td>System Error Indicator</td><td>Event Log</td><td>E-Mail</td><td>Call-Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td>✔</td><td></td><td>✔</td><td></td><td></td><td></td><td></td></tr>
</table>

Event Code: 120	
Message:	`Error detected while processing system management command.`
Severity:	Informational.
Explanation:	This event occurs when the switch receives a command from the management tool (HAFM) that does not meet specified boundary conditions. This may occur as a result of a network communication error. The switch rejects the command, then disconnects from the management tool to force error recovery processing. The management tool should immediately reconnect, and the operation can be retried.

Action:	No action required if this is an isolated event. If this event is persistent, perform a data collection operation for this switch and return the data to HP Services for analysis.						
Event Data:	None.						
Distribution:	Switch		HAFM Server			Host	
	Nonvolatile System Event Log	System Error Indicator	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔		✔				

Event Code: 121							
Message:	`Zone set activation failed. Zone set too large.`						
Severity:	Informational.						
Explanation:	This event occurs when the switch receives a zone set activation command from the management tool (HAFM) that exceed the size supported by the switch. The switch rejects the command, then disconnects from the management tool to force error recovery processing. The management tool should immediately reconnect, and the operation can be retried.						
Action:	Reduce the size of the zone set so it conforms to the limits specified in the user manual and retry the activation. Verify that the number of zones and zone members in the zone set are within the limits stated in the user manual, or try reducing the length of zone names.						
Event Data:	None.						
Distribution:	Switch		HAFM Server			Host	
	Nonvolatile System Event Log	System Error Indicator	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔		✔				

Power Supply Events (200 through 299)

Event Code: 200							
Message:	`Power supply AC voltage failure.`						
Severity:	Major.						
Explanation:	Alternating current (AC) input to the indicated power supply is disconnected or AC circuitry in the power supply failed. The second power supply assumes the full operating load for the switch.						
Action:	Ensure the power supply is connected to facility AC power, and verify operation of the facility power source. If the AC voltage does not recover (indicated by event code **203**), replace the failed power supply. Perform the data collection procedure and return the Zip disk and failed power supply to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 201							
Message:	`Power supply DC voltage failure.`						
Severity:	Major.						
Explanation:	Direct current (DC) circuitry in the power supply failed. The second power supply assumes the full operating load for the switch.						
Action:	Replace the failed power supply. Perform the data collection procedure and return the Zip disk and failed power supply to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 202	
Message:	`Power supply thermal failure.`
Severity:	Major.

Explanation:	The thermal sensor associated with a power supply indicates an overheat condition that shut down the power supply. The second power supply assumes the full operating load for the switch.						
Action:	Replace the failed power supply. Perform the data collection procedure and return the Zip disk and failed power supply to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 203							
Message:	`Power supply AC voltage recovery.`						
Severity:	Informational.						
Explanation:	AC voltage recovered for the power supply. Both power supplies adjust to share operating load for the switch.						
Action:	No action required.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 204	
Message:	`Power supply DC voltage recovery.`
Severity:	Informational.
Explanation:	DC voltage recovered for the power supply. Both power supplies adjust to share operating load for the switch.
Action:	No action required.
Event Data:	No supplementary data included with the event.

Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 206							
Message:	`Power supply removed.`						
Severity:	Informational.						
Explanation:	A power supply was removed while the Switch was powered on and operational. The second power supply assumes the full operating load for the switch.						
Action:	No action required or install an operational power supply.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 207							
Message:	`Power supply installed.`						
Severity:	Informational.						
Explanation:	A redundant power supply was installed with the switch powered on and operational. Both power supplies adjust to share operating load for the switch.						
Action:	No action required.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 208	
Message:	`Power supply false shutdown.`
Severity:	Major.

Explanation:	Switch operational firmware nearly shut down the indicated power supply as a result of failure or facility power loss or voltage fluctuation.						
Action:	Confirm operation of facility power. If subsequent power loss events occur, replace the failed power supply. Perform the data collection procedure and return the Zip disk and failed power supply to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Fan Module Events (300 through 399)

Event Code: 300							
Message:	`Cooling fan propeller failed.`						
Severity:	Major.						
Explanation:	One cooling fan (out of four) failed or is rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of the failed fan.						
Action:	Replace the indicated fan module.						
Event Data:	The first byte of event data (byte **0**) specifies the failed fan number.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 301	
Message:	`Cooling fan propeller failed.`
Severity:	Major.
Explanation:	Two cooling fans (out of four) failed or are rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of the failed fans.
Action:	Replace the indicated fan modules.
Event Data:	The first byte of event data (byte **0**) specifies the failed fan numbers.

Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 302							
Message:	`Cooling fan propeller failed.`						
Severity:	Major.						
Explanation:	Three cooling fans (out of four) failed or are rotating at insufficient angular velocity. The remaining fan is operational. The amber LED illuminates at the rear of the failed fans.						
Action:	Replace the indicated fan modules.						
Event Data:	The first byte of event data (byte **0**) specifies the failed fan numbers.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 305							
Message:	`Cooling fan propeller failed.`						
Severity:	Major.						
Explanation:	All four cooling fans failed or are rotating at insufficient angular velocity. The amber LED illuminates at the rear of the fan modules.						
Action:	Replace the fans						
Event Data:	The first byte of event data (byte **0**) specifies the failed fan numbers.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 310	
Message:	`Cooling fan propeller recovered.`
Severity:	Informational.

Explanation:	One cooling fan (out of four) recovered or the associated fan module was replaced. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte **0**) specifies the recovered fan number.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 311							
Message:	`Cooling fan propeller recovered.`						
Severity:	Informational.						
Explanation:	Two cooling fans (out of four) recovered or the associated fan modules were replaced. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte **0**) specifies the recovered fan numbers.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error Indicator	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 312							
Message:	`Cooling fan propeller recovered.`						
Severity:	Informational.						
Explanation:	Three cooling fans (out of four) recovered or the associated fan modules were replaced. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte **0**) specifies the recovered fan numbers.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 315							
Message:	`Cooling fan propeller recovered.`						
Severity:	Informational.						
Explanation:	All cooling fans recovered or the associated fan modules were replaced. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte **0**) specifies the recovered fan numbers.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

CTP2 Card Events (400 through 499)

The term CTP card refers to the main circuit board of the Edge Switch 2/32, not to a separate card that contains the CTP. The CTP is an integral part of the main circuit board.

Event Code: 400	
Message:	`Power-up diagnostics failure.`
Severity:	Major.
Explanation:	The CTP power-on self test diagnostics detected a faulty FRU as indicated in the event data.
Action:	Replace the faulty FRU with a functional FRU. Perform the data collection procedure for the switch using HAFM, and return the Zip disk and the faulty FRU to HP Services for analysis and repair.

<table>
<tr><td>Event Data:</td><td colspan="7">Byte 0: FRU code:
01 = LBA
02 = CTP
03 = SBAR
05 = Fan module
06 = Power supply
08-0F = Port module
Byte 1: Slot position
Byte 2: Device ID
Byte 3: Power-up error code (Internally defined) (stored in the faulty FRU EEPROM for analysis)
Bytes 4–7: Power-up data code (Internally defined) (stored in the faulty FRU EEPROM)</td></tr>
<tr><td rowspan="2">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Server</td><td colspan="2">Host</td></tr>
<tr><td>Nonvola-tile System Event Log</td><td>System Error Indicator</td><td>Event Log</td><td>E-Mail</td><td>Call-Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td></td><td>✔</td><td>✔</td><td>✔</td><td>✔</td><td>✔</td><td>✔</td><td></td></tr>
</table>

<table>
<tr><th colspan="8">Event Code: 410</th></tr>
<tr><td>Message:</td><td colspan="7"><tt>CTP card reset.</tt></td></tr>
<tr><td>Severity:</td><td colspan="7">Informational.</td></tr>
<tr><td>Explanation:</td><td colspan="7">The CTP card reset after a switch power-on, hardware IML, or software IPL. An IPL can be user-initiated at the switch- Product Manager application, or occur automatically after a firmware fault (event code 411). The event data indicates the type of reset.</td></tr>
<tr><td>Action:</td><td colspan="7">No action required.</td></tr>
<tr><td>Event Data:</td><td colspan="7">Byte 0 = reset type as follows: 00 = power-on or single CTP2 card hot-insert, 02 = IML, 04 = IPL,
08 = reset by other CTP2 card, 40 = partition switch, or 80 = dual CTP2 card hot-insert.</td></tr>
<tr><td rowspan="2">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Server</td><td colspan="2">Host</td></tr>
<tr><td>EWS Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td></td><td>✔</td><td></td><td>✔</td><td></td><td></td><td></td><td></td></tr>
</table>

Event Code: 411							
Message:	`Firmware fault occurred.`						
Severity:	Major.						
Explanation:	The firmware executing on the indicated CTP card encountered an unexpected operating condition and dumped its current operating state to FLASH memory for retrieval and analysis. All Fibre Channel connections to the switch are reset after the fault and IPL. Attached devices must re-login to the switch to resume operations. The dump file is automatically transferred from the switch to the HAFM server over the Ethernet LAN connection, where it is stored for later retrieval during the data collection operation.						
Action:	Perform the data collection procedure for this switch using HAFM, save the data file to the HAFM server Zip drive, and return the Zip disk to HP Services for analysis.						
Event Data:	Bytes **0–3 =** Fault identifier, least significant byte first (for example, event data 33 22 11 00). Bytes **4–7** = Fault identifier specific data. Bytes **8–11** = Fault identifier specific data.						
Distribution:	Switch		HAFM Server			Host	
	Nonvolatile System Event Log	System Error Indicator	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 421	
Message:	`Firmware download complete.`
Severity:	Informational.
Explanation:	A new version of the switch firmware was successfully downloaded from the HAFM server or from the Embedded Web Server.
Action:	No action required.

Event Data:	New firmware release level (ASCII) in the format: FF.MM.II BBBB. FF: Bytes **0–1** = Function release level. MM: Bytes **3–4** = Maintenance release level. II: Bytes **6–7** = Interim release level. BBBBB: Bytes **9–12** = Build ID. Example: 30 31 2E 30 32 2E 30 30 20 30 30 34 38 = Release 10.02.00 Build 0048. Notes: Release format punctuation is incorporated in data and formatted in ASCII. Only the first byte of word 3 is used. Data is an array of bytes eliminating any LSB/MSB considerations.						
Distribution:	Switch		HAFM Server			Host	
	Nonvola-tile System Event Log	System Error Indicator	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔		✔				

Event Code: 423							
Message:	`CTP firmware download initiated.`						
Severity:	Informational.						
Explanation:	The HAFM server initiated download of a new firmware version to the switch.						
Action:	No action required.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 430	
Message:	`Excessive Ethernet transmit errors.`
Severity:	Informational.

Explanation:	Transmit error counters for the CTP card Ethernet adapter (sum of all counters) exceeded a threshold. This does not indicate a CTP failure; it indicates a problem with the Ethernet cable, hub, or device on the same Ethernet segment. Event data counters are represented in hexadecimal format with the least significant byte first.						
Action:	Verify the Ethernet cable, hub, and other devices are properly connected and operational.						
Event Data:	Bytes **0** through **3** = sum of all transmit errors (**total_xmit_error**). Bytes **4** through **7** = frame count where Ethernet adapter does not detect carrier sense at preamble end (**loss_of_CRSs_cnt**). Bytes **8** through **11** = frame count where Ethernet adapter does not detect a collision within 64 bit times at transmission end (**SQE_error_cnt**). Bytes **12** through **15** = frame count where Ethernet adapter detects a collision more than 512 bit times after first preamble bit (**out_of_window_cnt**). Frame not transmitted. Bytes **16** through **19** = frame count where transmission is more than 26 ms (**jabber_cnt**). Frame not transmitted. Bytes **20** through **23** = frame count where Ethernet adapter encounters 16 collisions while attempting to transmit a frame (**16coll_cnt**). Frame not transmitted.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 431	
Message:	`Excessive Ethernet receive errors.`
Severity:	Informational.
Explanation:	Receive error counters for the CTP card Ethernet adapter (sum of all counters) exceeded a threshold. This does not indicate a CTP failure; it indicates a problem with the Ethernet cable, hub, or device on the same Ethernet segment. Event data counters are represented in hexadecimal format with the least significant byte first.
Action:	Verify the Ethernet cable, hub, and other devices are properly connected and operational.

Event Data:	Bytes **0** through **3** = sum of all receive errors (**total_recv_error**). Bytes **4** through **7** = frame count where received frame had from 1 to 7 bits after last received full byte (**dribble_bits_cnt**). CRC error counter updated but frame not processed. Bytes **8** through **11** = frame count where received frame had bad CRC (**CRC_error_cnt**). Frame not processed. Bytes **12** through **15** = frame count received with less than 64 bytes (**runt_cnt**). Broadcast frames count but do not contribute to threshold. Frame not processed. Bytes **16** through **19** = frame count received with more than 1518 bytes (**extra_data_cnt**). Broadcast frames count but do not contribute to threshold. Frame not processed.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 432							
Message:	`Ethernet adapter reset.`						
Severity:	Minor.						
Explanation:	The CTP card Ethernet adapter was reset in response to an internally detected error. A card failure is not indicated. The switch-to-HAFM server connection terminates, but automatically recovers after the reset.						
Action:	Perform the data collection procedure and return the Zip disk to HP support personnel.						
Event Data:	Bytes **0** through **3** = reason for adapter reset, least significant byte first (**reset_error_type**) **1** = completion notification for timed-out frame transmission.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 433	
Message:	`Non-recoverable Ethernet fault.`
Severity:	Major.

Explanation:	A non-recoverable error was detected on the CTP card Ethernet adapter and the LAN connection to the HAFM server terminated. All Fibre Channel switching functions remain unaffected. Because Ethernet communication is lost, no failure indication is externally reported.						
Action:	Replace the failed switch. Perform the data collection procedure and return the Zip disk and faulty switch to HP support personnel.						
Event Data:	Bytes **0** through **3** = LAN error type, where **01** = hard failure and **04** = registered fault. Bytes **4** through **7** = LAN error subtype. Bytes **8** through **11** = fault identifier.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔				✔	

Event Code: 440							
Message:	`Embedded Port hardware has failed.`						
Severity:	Major.						
Explanation:	The embedded port hardware detected an error.						
Action:	Replace the switch. Perform a data collection operation for the switch using HAFM, Save the data file to the HAFM server Zip drive, and return the failed CTP card and the Zip disk to HP Services for analysis and repair.						
Event Data:	Byte **0** = Slot Position. Byte **1** = Reason Code: 00 = TX clock loss. 01 = Solicited response parity error detected. 02 = Solicited response invalid error detected. 03 = High availability error threshold exceeded. Bytes **4–7** = Elapsed millisecond tick count. Bytes **8–11** = High availability error callout (internally defined).						
Distribution:	Switch		HAFM Server			Host	
	Nonvola-tile System Event Log	System Error Indicator	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

<table>
<tr><th colspan="8">Event Code: 442</th></tr>
<tr><td>Message:</td><td colspan="7">Embedded Port Anomaly Detected.</td></tr>
<tr><td>Severity:</td><td colspan="7">Informational.</td></tr>
<tr><td>Explanation:</td><td colspan="7">Indicates that the control processor has detected a deviation in the normal operation mode or operation status of the embedded port.</td></tr>
<tr><td>Action:</td><td colspan="7">No action required. There will be an additional event generated if the occurrence of this incident exceeds an error threshold resulting in a module or port failure.</td></tr>
<tr><td>Event Data:</td><td colspan="7">Word 0:
Byte 0 = Embedded port number.
Byte 1 = Reason Code (See following chart).
Word 1:
Byte 0–3 = Elapsed millisecond tick count.
Word 2:
Byte 0–1 = High availability error callout #1.
Byte 2–3 = High availability error callout #2.
Word 3:
Byte 0 = Detecting port.
Byte 1 = Connected port.
Byte 3 = Reserved.
Word 4:
Byte 0–1 = High availability error callout #3.
Byte 2–3 = High availability error callout #4.</td></tr>
<tr><td rowspan="3">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Server</td><td colspan="2">Host</td></tr>
<tr><td>Nonvola-tile System Event Log</td><td>System Error Indicator</td><td>Event Log</td><td>E-Mail</td><td>Call-Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td>✔</td><td></td><td>✔</td><td></td><td></td><td></td><td></td></tr>
</table>

Event #442 Anomaly Reason Codes		
Reason Code	**Description**	**Additional Data**
0x00	Utility bus error to SBAR	HA Error Callouts (Words 2 and 4)
0x01	Utility bus error to Port Module	HA Error Callouts (Words 2 and 4)
0x02	Reserved	HA Error Callouts (Words 2 and 4)

0x03	SBAR module detected utility bus parity error	HA Error Callouts (Words 2 and 4)
0x04	Port module detected utility bus parity error	HA Error Callouts (Words 2 and 4)
0x05	SBAR module detected clock frequency error	HA Error Callouts (Words 2 and 4)
0x06	Port module detected clock frequency error	HA Error Callouts (Words 2 and 4)
0x07	SBAR module detected CTP interface signal error	HA Error Callouts (Words 2 and 4)
0x08	Port module detected CTP interface signal error	HA Error Callouts (Words 2 and 4)
0x09	SBAR Module detected external parity error	HA Error Callouts (Words 2 and 4)
0x0A	Port Module detected external parity error	HA Error Callouts (Words 2 and 4)
0x0B	SBAR Module detected lost of system clock	HA Error Callouts (Words 2 and 4)
0x0C	Port Module detected lost of system clock	HA Error Callouts (Words 2 and 4)
0x0D	SBAR detected invalid request from port	HA Error Callouts (Words 2 and 4)
0x0E	Internal SBAR time out	HA Error Callouts (Words 2 and 4)
0x0F	Internal SBAR parity error	HA Error Callouts (Words 2 and 4)
0x10	User port internal protocol error	HA Error Callouts (Words 2 and 4)
0x11	User port internal parity error	HA Error Callouts (Words 2 and 4)
0x12	User port internal buffer range error	HA Error Callouts (Words 2 and 4)
0x13	User port internal time out #1	HA Error Callouts (Words 2 and 4)
0x14	User port internal time out #2	HA Error Callouts (Words 2 and 4)
0x15	User port internal frame error—bad delimiter	HA Error Callouts (Words 2 and 4)
0x16	User port internal frame error—CRC	HA Error Callouts (Words 2 and 4)
0x17	User port internal frame error—invalid size	HA Error Callouts (Words 2 and 4)

0x18	User port internal frame error—long frame	HA Error Callouts (Words 2 and 4)
0x19	User port internal frame error—short frame	HA Error Callouts (Words 2 and 4)
0x1A	User port internal parity error	HA Error Callouts (Words 2 and 4)
0x1B	Buffer error	HA Error Callouts (Words 2 and 4)
0x1C	User port detected unexpected frame transmission	HA Error Callouts (Words 2 and 4)
0x1D	User port internal frame error—invalid trailer	HA Error Callouts (Words 2 and 4)
0x1E	User port detected frame internal integrity error	HA Error Callouts (Words 2 and 4)
0x1F	Internal connection time out	HA Error Callouts (Words 2 and 4)
0x20	User port detected elastic store error	HA Error Callouts (Words 2 and 4)
0x21	User port detected trailer parity error	HA Error Callouts (Words 2 and 4)
0x22	User port detected internal frame error—long frame	HA Error Callouts (Words 2 and 4)
0x23	Port detected SBAR response error	HA Error Callouts (Words 2 and 4)
0x24	User port detected clock error	HA Error Callouts (Words 2 and 4)
0x25	Port module internal address bus error	HA Error Callouts (Words 2 and 4)
0x26	User module internal data bus error	HA Error Callouts (Words 2 and 4)
0x27	User Port detected invalid address	HA Error Callouts (Words 2 and 4)
0x28	Embedded port detected frame integrity error	HA Error Callouts (Words 2 and 4)
0x29	Embedded port detected frame error—non-parity	HA Error Callouts (Words 2 and 4)
0x2A	Embedded port detected frame error—parity	HA Error Callouts (Words 2 and 4)
0x2B	Embedded port detected invalid SBAR response	HA Error Callouts (Words 2 and 4)

0x2C	Embedded port detected receive frame parity error	HA Error Callouts (Words 2 and 4)
0x2D	Embedded port detected connection time out	HA Error Callouts (Words 2 and 4)
0x2E	Embedded port detected receive fame overrun error	HA Error Callouts (Words 2 and 4)
0x2F	Embedded port detected frame transmit error	HA Error Callouts (Words 2 and 4)
0x30	Embedded port detected request time out	HA Error Callouts (Words 2 and 4)
0x31	Embedded port internal parity error	HA Error Callouts (Words 2 and 4)
0x32	Reserved (Engineering use only)	HA Error Callouts (Words 2 and 4)
0x33	Health Check—port failed busy bit clear	HA Error Callouts (Words 2 and 4)
0x34	Health Check—port detected bit synchronization error	HA Error Callouts (Words 2 and 4)
0x35	Diagnostic port test failure	HA Error Callouts (Words 2 and 4)
0x36	Embedded Port detected internal frame error—invalid trailer	HA Error Callouts (Words 2 and 4)
0x37	SBAR detected request out of range error	HA Error Callouts (Words 2 and 4)
0x38	User port internal time-out #3	HA Error Callouts (Words 2 and 4)
0x39	Embedded Port detected CRC Error	HA Error Callouts (Words 2 and 4)
0x3A	User port internal protocol error—Unsolicited response	HA Error Callouts (Words 2 and 4)
0x3B	User port detected frame error—Undeliverable frame	HA Error Callouts (Words 2 and 4)
0x3C	User port detected transmission rate discrepancy	HA Error Callouts (Words 2 and 4)
0x3D	User port detected transmission rate inconsistent mode	HA Error Callouts (Words 2 and 4)
0x3E	User port internal protocol error—Credit out of sync	HA Error Callouts (Words 2 and 4)
0x3F	Reserved	

0x40	SBAR detected request out of range error	HA Error Callouts (Words 2 and 4)
0x41	Reserved	
0x42	User egress port detected frame transmission error	HA Error Callouts (Words 2 and 4)
0x43	User ingress port detected internal time-out	HA Error Callouts (Words 2 and 4)
0x44	Reserved	HA Error Callouts (Words 2 and 4)
0x45	User egress port detected frame internal integrity error	HA Error Callouts (Words 2 and 4)
0x46	User egress port detected internal protocol error.	HA Error Callouts (Words 2 and 4)
0x47	User port detected internal frame length error	HA Error Callouts (Words 2 and 4)
0x48	User port detected internal buffer error	HA Error Callouts (Words 2 and 4)
0x49	User port detected internal queue protocol error.	HA Error Callouts (Words 2 and 4)
0x4A-0xFF		

Event Code: 460	
Message:	`Management request out of range.`
Severity:	Informational
Explanation:	This event occurs when requests passed from the managing tool (generally HAFM) to the switch do not meet data boundary specifications. This event is most likely to be triggered if a user attempt to activate a zone set that is larger than the maximum defined zone set size.
Action:	The switch found request data from the management tool to be larger or smaller than expected. The connection to the management tool will be temporarily lost. After the link is re-established, verify that all information changed in the managing tool is within the specified ranges. For example, verify that the zones and zone members in a zone set fall within the limits stated in the user manual. Try sending the request again.
Event Data:	None

Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Port Events (500 through 599)

In the Edge Switch 2/32, ports are not included on separate assemblies (UPM cards), therefore are not FRUs. Ports are an integral part of the switch's main circuit board. UPM card events apply to a single port as indicated by byte 13 of event data.

Event Code: 502							
Message:	`Port module anomaly has been detected.`						
Severity:	Informational.						
Explanation:	Indicates that the control processor has detected a deviation in the normal operating mode or operating status of the indicated four-port hardware module.						
Action:	No action required. There will be an additional event code generated (504) if this occurrence exceeds an error threshold, which results in a subsequent port module failure.						
Event Data:	Byte **0** = Slot position. Byte **1** = Anomaly reason code (See following chart): 0x00 = Common logic error. 0x01 = ASIC common error. Bytes **4–7** = Elapsed millisecond tick count. Bytes **8–9** = High availability error callout #1. Bytes **10–11** = High availability error callout #2. Byte **12** = Detecting port. Byte **13** = Connected port. Byte **14** = Participating SBAR. Bytes **16–17** = High availability error callout #3. Bytes **18–19** = High availability error callout #4.						
Distribution:	Switch		HAFM Server			Host	
	Nonvolatile System Event Log	System Error Indicator	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔		✔				

Event #502 Anomaly Reason Codes		
Reason Code	**Description**	**Additional Data**
0x00	Utility bus error to SBAR	HA Error Callouts (Words 2 and 4)
0x01	Utility bus error to Port Module	HA Error Callouts (Words 2 and 4)
0x02	Reserved	HA Error Callouts (Words 2 and 4)
0x03	SBAR module detected utility bus parity error	HA Error Callouts (Words 2 and 4)
0x04	Port module detected utility bus parity error	HA Error Callouts (Words 2 and 4)
0x05	SBAR module detected clock frequency error	HA Error Callouts (Words 2 and 4)
0x06	Port module detected clock frequency error	HA Error Callouts (Words 2 and 4)
0x07	SBAR module detected CTP interface signal error	HA Error Callouts (Words 2 and 4)
0x08	Port module detected CTP interface signal error	HA Error Callouts (Words 2 and 4)
0x09	SBAR Module detected external parity error	HA Error Callouts (Words 2 and 4)
0x0A	Port Module detected external parity error	HA Error Callouts (Words 2 and 4)
0x0B	SBAR Module detected lost of system clock	HA Error Callouts (Words 2 and 4)
0x0C	Port Module detected lost of system clock	HA Error Callouts (Words 2 and 4)
0x0D	SBAR detected invalid request from port	HA Error Callouts (Words 2 and 4)
0x0E	Internal SBAR time out	HA Error Callouts (Words 2 and 4)
0x0F	Internal SBAR parity error	HA Error Callouts (Words 2 and 4)
0x10	User port internal protocol error	HA Error Callouts (Words 2 and 4)
0x11	User port internal parity error	HA Error Callouts (Words 2 and 4)
0x12	User port internal buffer range error	HA Error Callouts (Words 2 and 4)

0x13	User port internal time out #1	HA Error Callouts (Words 2 and 4)
0x14	User port internal time out #2	HA Error Callouts (Words 2 and 4)
0x15	User port internal frame error—bad delimiter	HA Error Callouts (Words 2 and 4)
0x16	User port internal frame error—CRC	HA Error Callouts (Words 2 and 4)
0x17	User port internal frame error—invalid size	HA Error Callouts (Words 2 and 4)
0x18	User port internal frame error—long frame	HA Error Callouts (Words 2 and 4)
0x19	User port internal frame error—short frame	HA Error Callouts (Words 2 and 4)
0x1A	User port internal parity error	HA Error Callouts (Words 2 and 4)
0x1B	Buffer error	HA Error Callouts (Words 2 and 4)
0x1C	User port detected unexpected frame transmission	HA Error Callouts (Words 2 and 4)
0x1D	User port internal frame error—invalid trailer	HA Error Callouts (Words 2 and 4)
0x1E	User port detected frame internal integrity error	HA Error Callouts (Words 2 and 4)
0x1F	Internal connection time out	HA Error Callouts (Words 2 and 4)
0x20	User port detected elastic store error	HA Error Callouts (Words 2 and 4)
0x21	User port detected trailer parity error	HA Error Callouts (Words 2 and 4)
0x22	User port detected internal frame error—long frame	HA Error Callouts (Words 2 and 4)
0x23	Port detected SBAR response error	HA Error Callouts (Words 2 and 4)
0x24	User port detected clock error	HA Error Callouts (Words 2 and 4)
0x25	Port module internal address bus error	HA Error Callouts (Words 2 and 4)
0x26	User module internal data bus error	HA Error Callouts (Words 2 and 4)
0x27	User Port detected invalid address	HA Error Callouts (Words 2 and 4)
0x28	Embedded port detected frame integrity error	HA Error Callouts (Words 2 and 4)

0x29	Embedded port detected frame error—non-parity	HA Error Callouts (Words 2 and 4)
0x2A	Embedded port detected frame error—parity	HA Error Callouts (Words 2 and 4)
0x2B	Embedded port detected invalid SBAR response	HA Error Callouts (Words 2 and 4)
0x2C	Embedded port detected receive frame parity error	HA Error Callouts (Words 2 and 4)
0x2D	Embedded port detected connection time out	HA Error Callouts (Words 2 and 4)
0x2E	Embedded port detected receive fame overrun error	HA Error Callouts (Words 2 and 4)
0x2F	Embedded port detected frame transmit error	HA Error Callouts (Words 2 and 4)
0x30	Embedded port detected request time out	HA Error Callouts (Words 2 and 4)
0x31	Embedded port internal parity error	HA Error Callouts (Words 2 and 4)
0x32	Reserved (Engineering use only)	HA Error Callouts (Words 2 and 4)
0x33	Health Check—port failed busy bit clear	HA Error Callouts (Words 2 and 4)
0x34	Health Check—port detected bit synchronization error	HA Error Callouts (Words 2 and 4)
0x35	Diagnostic port test failure	HA Error Callouts (Words 2 and 4)
0x36	Embedded Port detected internal frame error—invalid trailer	HA Error Callouts (Words 2 and 4)
0x37	SBAR detected request out of range error	HA Error Callouts (Words 2 and 4)
0x38	User port internal time-out #3	HA Error Callouts (Words 2 and 4)
0x39	Embedded Port detected CRC Error	HA Error Callouts (Words 2 and 4)
0x3A	User port internal protocol error—Unsolicited response	HA Error Callouts (Words 2 and 4)
0x3B	User port detected frame error—Undeliverable frame	HA Error Callouts (Words 2 and 4)

0x3C	User port detected transmission rate discrepancy	HA Error Callouts (Words 2 and 4)
0x3D	User port detected transmission rate inconsistent mode	HA Error Callouts (Words 2 and 4)
0x3E	User port internal protocol error—Credit out of sync	HA Error Callouts (Words 2 and 4)
0x3F	Reserved	
0x40	SBAR detected request out of range error	HA Error Callouts (Words 2 and 4)
0x41	Reserved	
0x42	User egress port detected frame transmission error	HA Error Callouts (Words 2 and 4)
0x43	User ingress port detected internal timeout	HA Error Callouts (Words 2 and 4)
0x44	Reserved	HA Error Callouts (Words 2 and 4)
0x45	User egress port detected frame internal integrity error	HA Error Callouts (Words 2 and 4)
0x46	User egress port detected internal protocol error.	HA Error Callouts (Words 2 and 4)
0x47	User port detected internal frame length error	HA Error Callouts (Words 2 and 4)
0x48	User port detected internal buffer error	HA Error Callouts (Words 2 and 4)
0x49	User port detected internal queue protocol error.	HA Error Callouts (Words 2 and 4)
0x4A-0xFF		

Event Code: 504	
Message:	`Port module failure.`
Severity:	Major.
Explanation:	A failure associated with a four-port hardware module has been detected. The amber Service Required LED is illuminated on each of the module's four contiguous ports.

Action:	Perform data collection procedure for the switch using HAFM, save the data file to the HAFM server Zip drive. Return the Zip disk to HP Services for analysis. Perform a system power-on reset. If the problem persists, replace the switch.
Event Data:	Byte **0** = Slot position. Byte **1** = Reason code: 00 = Operator requested with debug command. 02 = Initialization failure. 03 = Hot plug/power up diagnostics failure acknowledgment. 04 = Board ready time-out. 05 = Read of module ID failed. 06 = Statistical error threshold reached. 07 = Communication with hardware is irregular or nonexistent. Bytes **4–7** = Elapsed millisecond tick count. Bytes **8–11** = Reason code specific data #1 (Internally defined).

Distribution:	Switch		HAFM Server			Host	
	Nonvolatile System Event Log	System Error Indicator	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 505	
Message:	`Port module revision not supported.`
Severity:	Minor.
Explanation:	The specified port hardware module is not supported by the existing firmware. The associated ports will appear uninstalled to system software.
Action:	Ensure that the switch model supports the operating firmware. If the firmware provides support for the indicated model, perform a data collection operation for this switch using HAFM, saving the data file to the HAFM server Zip drive. If the problem persists following a system power-on reset, replace the switch and return both the failing switch and the Zip disk to HP Services for analysis and repair.

<table>
<tr><td>Event Data:</td><td colspan="7">Byte 0 = Slot position.
Byte 1 = Reason code:
00 = Unrecognized board ID.
01 = FPM in an intolerant (2-gig) switch.
02 = FPM in an unsupported switch.
Bytes 4–7 = Elapsed millisecond tick count.</td></tr>
<tr><td rowspan="2">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Server</td><td colspan="2">Host</td></tr>
<tr><td>Nonvolatile System Event Log</td><td>System Error Indicator</td><td>Event Log</td><td>E-Mail</td><td>Call-Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td></td><td>✔</td><td></td><td>✔</td><td></td><td></td><td></td><td></td></tr>
</table>

Event Code: 506	
Message:	`Fibre Channel port failure.`
Severity:	Major.
Explanation:	One of the four ports on a single port module has failed and has been taken out of service. Normally the amber Service Required LED on the corresponding port is illuminated to indicate which port has failed. All other ports on the module remain operational if their respective Service Required LEDs are off.
Action:	Perform a data collection procedure for this switch using HAFM, save the data file to the HAFM server Zip drive and return the Zip disk to HP Services for analysis. Perform a system power-on reset. If the problem persists, replace the switch. A failed port may also be recovered by performing a port reset using HAFM or the Web interface, however newly detected errors may result in the port failing again.

Event Data:	Byte **0** = Port number (00 — 3F). Byte **1** = Reason code: 00 = Operator requested with debug command. 01 = Hot plug, power up or online diagnostics failure acknowledgment. 02 = Initialization failure. 03 = High availability error threshold reached. Bytes **4–7** = Elapsed millisecond tick count. Bytes **8–11** = Reason code specific (internally defined). Byte **12** = Connector type: 00 = Unknown. 01-06 = Reserved. 07 = LC connector. 08 = MT-RJ connector. 09 = MU connector. Bytes **13–14** = Transmitter technology: 0200 = Longwave laser (LC). 0040 = Shortwave laser. 0020 = Shortwave laser with OFC. 0010 = Longwave laser (LL). 0008 = Long distance. Byte **15** = Distance capabilities” 80 = Very long. 40 = Short. 20 = Intermediate. 10 = Long. Byte **16** = Supported transmission media: 08 = Multi-mode 62.5. 04 = Multi-mode 50. 01 = Single mode. Byte **17** = Speed capabilities: 10 = 400 Mbytes per second. 04 = 200 Mbytes per second. 01 = 100 Mbytes per second.

Distribution:	Switch		HAFM Server			Host	
	Nonvolatile System Event Log	System Error Indicator	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 507	
Message:	`Loopback diagnostics port failure.`
Severity:	Informational.
Explanation:	A loopback diagnostic test detected a port failure. Loopback diagnostics are initiated through HAFM or as a result of the hot insertion of a port module (on supported models).
Action:	No action required. There will be an additional event generated (506) if the diagnostic failure incident results in a port failure.

<table>
<tr><td>Event Data:</td><td colspan="7">Byte 0 = Port number (00-8F).
Byte 1 = Failure reason code:
0x00 = Unable to generate test frame.
0x01 = Unable to send test frame.
0x02 = Timed out waiting for test frame.
0x00 = Received frame contained invalid/corrupt data.
0x04 = External wrap test requires active link.
0x05 = Routing table test failed.
0x06 = No bit sync achieved.
0x07 = VC rare event status register is set.
0x10 = Port’s maximum speed is less than the backplane speed.
0x11 = Unrecognized module/chip revision.
0x12 = SERDES read failed.
Bytes 4–7 = Elapsed millisecond tick count.
Byte 8 = Test type:
0x01 = Internal wrap.
0x02 = External wrap.
0x03 = Hotplug.
0x05 = Internal BIST.
0x06 = External BIST.
0x08 = Internal EMC loopback.
0x09 = External EMC loopback.
0x0A = Internal system loopback.
0x0B = External system loopback.
Bytes 12–13 = SB rare event register contents.
Bytes 14–15 = BB rare event register contents.
Bytes 16–17 = RD rare event register contents.
Bytes 18–19 = FE rare event register contents.
Bytes 20–21 = QM rare event register contents.
Bytes 22 = WR rare event register contents.
Bytes 23 = RD rare event register contents.</td></tr>
<tr><td rowspan="2">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Server</td><td colspan="2">Host</td></tr>
<tr><td>Nonvola-tile System Event Log</td><td>System Error Indicator</td><td>Event Log</td><td>E-Mail</td><td>Call-Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td></td><td>✔</td><td></td><td>✔</td><td></td><td></td><td></td><td></td></tr>
</table>

<table>
<tr><th colspan="8">Event Code: 508</th></tr>
<tr><td>Message:</td><td colspan="7">Fibre Channel port anomaly detected.</td></tr>
<tr><td>Severity:</td><td colspan="7">Informational.</td></tr>
<tr><td>Explanation:</td><td colspan="7">Indicates that the control processor has detected a deviation in the normal operating mode or operating status of the indicated port.</td></tr>
<tr><td>Action:</td><td colspan="7">No action required. There will be an additional event generated (506) if the diagnostic failure incident results in a port failure.</td></tr>
<tr><td>Event Data:</td><td colspan="7">Byte 0 = Port number (00-8F).
Byte 1 = Anomaly reason code (See following chart).
Bytes 4–7 = Elapsed millisecond tick count.
Bytes 8–9 = High availability error callout #1 (Internally defined).
Bytes 10–11 = High availability error callout #2 (Internally defined).
Byte 12 = Detecting port.
Byte 13 = Connected port.
Byte 14 = Participating SBAR.
Bytes 16–17 = High Availability error callout #3 (Internally defined).
Bytes 18–19 = High Availability error callout #4 (Internally defined).</td></tr>
<tr><td rowspan="2">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Server</td><td colspan="2">Host</td></tr>
<tr><td>Nonvola-tile System Event Log</td><td>System Error Indicator</td><td>Event Log</td><td>E-Mail</td><td>Call-Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td></td><td>✔</td><td></td><td>✔</td><td></td><td></td><td></td><td></td></tr>
</table>

Event #508 Anomaly Reason Codes		
Reason Code	**Description**	**Additional Data**
0x00	Utility bus error to SBAR	HA Error Callouts (Words 2 and 4)
0x01	Utility bus error to Port Module	HA Error Callouts (Words 2 and 4)
0x02	Reserved	HA Error Callouts (Words 2 and 4)
0x03	SBAR module detected utility bus parity error	HA Error Callouts (Words 2 and 4)
0x04	Port module detected utility bus parity error	HA Error Callouts (Words 2 and 4)

0x05	SBAR module detected clock frequency error	HA Error Callouts (Words 2 and 4)
0x06	Port module detected clock frequency error	HA Error Callouts (Words 2 and 4)
0x07	SBAR module detected CTP interface signal error	HA Error Callouts (Words 2 and 4)
0x08	Port module detected CTP interface signal error	HA Error Callouts (Words 2 and 4)
0x09	SBAR Module detected external parity error	HA Error Callouts (Words 2 and 4)
0x0A	Port Module detected external parity error	HA Error Callouts (Words 2 and 4)
0x0B	SBAR Module detected lost of system clock	HA Error Callouts (Words 2 and 4)
0x0C	Port Module detected lost of system clock	HA Error Callouts (Words 2 and 4)
0x0D	SBAR detected invalid request from port	HA Error Callouts (Words 2 and 4)
0x0E	Internal SBAR time out	HA Error Callouts (Words 2 and 4)
0x0F	Internal SBAR parity error	HA Error Callouts (Words 2 and 4)
0x10	User port internal protocol error	HA Error Callouts (Words 2 and 4)
0x11	User port internal parity error	HA Error Callouts (Words 2 and 4)
0x12	User port internal buffer range error	HA Error Callouts (Words 2 and 4)
0x13	User port internal time out #1	HA Error Callouts (Words 2 and 4)
0x14	User port internal time out #2	HA Error Callouts (Words 2 and 4)
0x15	User port internal frame error—bad delimiter	HA Error Callouts (Words 2 and 4)
0x16	User port internal frame error—CRC	HA Error Callouts (Words 2 and 4)
0x17	User port internal frame error—invalid size	HA Error Callouts (Words 2 and 4)
0x18	User port internal frame error—long frame	HA Error Callouts (Words 2 and 4)
0x19	User port internal frame error—short frame	HA Error Callouts (Words 2 and 4)

0x1A	User port internal parity error	HA Error Callouts (Words 2 and 4)
0x1B	Buffer error	HA Error Callouts (Words 2 and 4)
0x1C	User port detected unexpected frame transmission	HA Error Callouts (Words 2 and 4)
0x1D	User port internal frame error—invalid trailer	HA Error Callouts (Words 2 and 4)
0x1E	User port detected frame internal integrity error	HA Error Callouts (Words 2 and 4)
0x1F	Internal connection time out	HA Error Callouts (Words 2 and 4)
0x20	User port detected elastic store error	HA Error Callouts (Words 2 and 4)
0x21	User port detected trailer parity error	HA Error Callouts (Words 2 and 4)
0x22	User port detected internal frame error—long frame	HA Error Callouts (Words 2 and 4)
0x23	Port detected SBAR response error	HA Error Callouts (Words 2 and 4)
0x24	User port detected clock error	HA Error Callouts (Words 2 and 4)
0x25	Port module internal address bus error	HA Error Callouts (Words 2 and 4)
0x26	User module internal data bus error	HA Error Callouts (Words 2 and 4)
0x27	User Port detected invalid address	HA Error Callouts (Words 2 and 4)
0x28	Embedded port detected frame integrity error	HA Error Callouts (Words 2 and 4)
0x29	Embedded port detected frame error—non-parity	HA Error Callouts (Words 2 and 4)
0x2A	Embedded port detected frame error—parity	HA Error Callouts (Words 2 and 4)
0x2B	Embedded port detected invalid SBAR response	HA Error Callouts (Words 2 and 4)
0x2C	Embedded port detected receive frame parity error	HA Error Callouts (Words 2 and 4)
0x2D	Embedded port detected connection time out	HA Error Callouts (Words 2 and 4)

0x2E	Embedded port detected receive fame overrun error	HA Error Callouts (Words 2 and 4)
0x2F	Embedded port detected frame transmit error	HA Error Callouts (Words 2 and 4)
0x30	Embedded port detected request time out	HA Error Callouts (Words 2 and 4)
0x31	Embedded port internal parity error	HA Error Callouts (Words 2 and 4)
0x32	Reserved (Engineering use only)	HA Error Callouts (Words 2 and 4)
0x33	Health Check—port failed busy bit clear	HA Error Callouts (Words 2 and 4)
0x34	Health Check—port detected bit synchronization error	HA Error Callouts (Words 2 and 4)
0x35	Diagnostic port test failure	HA Error Callouts (Words 2 and 4)
0x36	Embedded Port detected internal frame error—invalid trailer	HA Error Callouts (Words 2 and 4)
0x37	SBAR detected request out of range error	HA Error Callouts (Words 2 and 4)
0x38	User port internal time-out #3	HA Error Callouts (Words 2 and 4)
0x39	Embedded Port detected CRC Error	HA Error Callouts (Words 2 and 4)
0x3A	User port internal protocol error—Unsolicited response	HA Error Callouts (Words 2 and 4)
0x3B	User port detected frame error—Undeliverable frame	HA Error Callouts (Words 2 and 4)
0x3C	User port detected transmission rate discrepancy	HA Error Callouts (Words 2 and 4)
0x3D	User port detected transmission rate inconsistent mode	HA Error Callouts (Words 2 and 4)
0x3E	User port internal protocol error—Credit out of sync	HA Error Callouts (Words 2 and 4)
0x3F	Reserved	
0x40	SBAR detected request out of range error	HA Error Callouts (Words 2 and 4)
0x41	Reserved	

0x42	User egress port detected frame transmission error	HA Error Callouts (Words 2 and 4)
0x43	User ingress port detected internal time-out	HA Error Callouts (Words 2 and 4)
0x44	Reserved	HA Error Callouts (Words 2 and 4)
0x45	User egress port detected frame internal integrity error	HA Error Callouts (Words 2 and 4)
0x46	User egress port detected internal protocol error.	HA Error Callouts (Words 2 and 4)
0x47	User port detected internal frame length error	HA Error Callouts (Words 2 and 4)
0x48	User port detected internal buffer error	HA Error Callouts (Words 2 and 4)
0x49	User port detected internal queue protocol error.	HA Error Callouts (Words 2 and 4)
0x4A-0xFF		

Event Code: 510							
Message:	`SFP optical transceiver hot-insertion initiated.`						
Severity:	Informational.						
Explanation:	Installation of a small form factor pluggable (SFP) optical transceiver was initiated with the switch powered on and operational. The event indicates that operational firmware detected the presence of the transceiver.						
Action:	No action required.						
Event Data:	Byte **0** = port number (**00** through **63**). Bytes **4** through **7** = elapsed millisecond tick count.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 512	
Message:	`SFP optical transceiver nonfatal error.`
Severity:	Minor.

Explanation:	Switch firmware detected an SFP optical transceiver non-fatal error.						
Action:	Replace the failed transceiver with a functional transceiver of the same type.						
Event Data:	Byte **0** = port number (**00** through **63**). Byte **1** = engineering reason code. Bytes **4** through **7** = elapsed millisecond tick count.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 513							
Message:	`SFP optical transceiver hot-removal completed.`						
Severity:	Informational.						
Explanation:	A SFP optical transceiver was removed while the switch was powered on and operational.						
Action:	No action required.						
Event Data:	Byte **0** = port number (**00** through **63**). Bytes **4** through **7** = elapsed millisecond tick count.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Event Code: 514	
Message:	`SFP optical transceiver failure.`
Severity:	Major.
Explanation:	A SFP optical transceiver failed. The amber LED corresponding to the port illuminates to indicate the failure. Other ports remain operational if their LEDs are extinguished.
Action:	Replace the failed transceiver with a functional transceiver of the same type.
Event Data:	Byte **0** = port number (**00** through **63**). Byte **1** = engineering reason code. Bytes **4** through **7** = elapsed millisecond tick count.

Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 581							
Message:	`Implicit incident.`						
Severity:	Major.						
Explanation:	A condition caused by an event known to have occurred within the incident node has been recognized by the incident node. The condition affects the attached link in such a way that it may cause a link incident to be recognized by the attached node.						
Action:	A Link-incident Record (LIR) is generated and sent to the host using the Link-Incident reporting procedure defined in the T11/99-017v0 document. If, after fault isolation is performed by the host, it is determined that the incident is because of a port failure, perform a data collection procedure for this switch using HAFM, save the data file to the HAFM server Zip drive, and return the Zip disk to HP Services for analysis.						
Event Data:	Byte **0** = Port number (00-8F). Bytes **4–7** = Elapsed millisecond tick count.						
Distribution:	Switch		HAFM Server			Host	
	Nonvolatile System Event Log	System Error Indicator	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
			✔				✔

Event Code: 582	
Message:	`Bit-error threshold exceeded.`
Severity:	Major.
Explanation:	The number of code violation errors recognized by the incident node has exceeded a threshold (see FC-PH clause 5.1).

Action:	A Link-incident Record (LIR) is generated and sent to the host using the Link-Incident reporting procedure defined in the T11/99-017v0 document. If, after fault isolation is performed by the host, it is determined that the incident is because of a port failure, perform a data collection procedure for this switch using HAFM, save the data file to the HAFM server Zip drive, and return the Zip disk to HP Services for analysis.						
Event Data:	Byte **0** = Port number (00-8F). Bytes **4–7** = Elapsed millisecond tick count.						
Distribution:	Switch		HAFM Server			Host	
	Nonvolatile System Event Log	System Error Indicator	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
			✔				✔

Event Code: 583	
Message:	`Loss-of —signal or loss-of-synchronization.`
Severity:	Major.
Explanation:	A loss-of-synchronization condition has been recognized by the incident node and it has persisted for more than the R_T_TOV timeout period. A loss-of-signal condition has been recognized by the incident node (see FC-PH clause 16.4.2).
Action:	A link-incident record (LIR) is generated and sent to the host using the Link-Incident reporting procedure defined in the T11/99-017v0 document. If, after fault isolation is performed by the host, it is determined that the incident is because of a port failure, perform a data collection procedure for this switch using HAFM, save the data file to the HAFM server Zip drive, and return the Zip disk to HP Services for analysis.

<table>
<tr><td>Event Data:</td><td colspan="7">Byte 0 = Port number (00-0F).
Bytes 4–7 = Elapsed millisecond tick count.
Bytes 8–11 = Port state indicators:
0x00 = Active.
0x01 = OLIB.
0x05 = LR1.
0x06 = LR2.
0x07 = LR3.
0x09 = LF2.
0x0A = LF1.
0x0C = OL1A.
0x0D = OL1C.
0x0E = OL2.
0x0F = OL3.</td></tr>
<tr><td rowspan="2">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Server</td><td colspan="2">Host</td></tr>
<tr><td>Nonvola-tile System Event Log</td><td>System Error Indicator</td><td>Event Log</td><td>E-Mail</td><td>Call-Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td></td><td></td><td>✔</td><td></td><td></td><td></td><td>✔</td></tr>
</table>

Event Code: 584	
Message:	`Not Operational primitive sequence (NOS) received.`
Severity:	Major.
Explanation:	The Not-Operational Primitive Sequence (NOS) has been recognized by the incident node (see FC-PH clause 16.5.3.2).
Action:	A Link-incident Record (LIR) is generated and sent to the host using the link-incident reporting procedure defined in the T11/99-017v0 document. If, after fault isolation is performed by the host, it is determined that the incident is because of a port failure, perform a data collection procedure for this switch using HAFM, Save the data file to the HAFM server Zip drive, and return Zip disk to HP Services for analysis.

Event Data:	Byte **0** = Port number (00-8F). Bytes **4–7** = Elapsed millisecond tick count. Bytes **8–11** = Port state indicators: 0x00 = Active. 0x01 = OLIB. 0x05 = LR1. 0x06 = LR2. 0x07 = LR3. 0x09 = LF2. 0x0A = LF1. 0x0C = OL1A. 0x0D = OL1C. 0x0E = OL2. 0x0F = OL3.						
Distribution:	Switch		HAFM Server			Host	
	Nonvola-tile System Event Log	System Error Indicator	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
			✔				✔

Event Code: 585	
Message:	`Primitive sequence time-out.`
Severity:	Major.
Explanation:	The incident node has recognized either a Link-Reset-Protocol (LR) timeout (see FC-PH clauses 16.5.2.1 and 16.5.2.3) or a timeout when timing for the appropriate response while in NOS Receive state and after NOS is no longer recognized (see FC-PH clause 16.5.3.2).
Action:	A link-incident record (LIR) is generated and sent to the host using the link-incident reporting procedure defined in the T11/99-017v0 document. If, after fault isolation is performed by the host, it is determined that the incident is because of a port failure, perform a data collection procedure for this switch using HAFM, Save the data file to the HAFM server Zip drive, and return the Zip disk to HP Services for analysis.

<table>
<tr><td>Event Data:</td><td colspan="7">Byte 0 = Port number (00-8F).
Bytes 4–7 = Elapsed millisecond tick count.
Bytes 8–11 = Port state indicators:
0x00 = Active.
0x01 = OLIB.
0x05 = LR1.
0x06 = LR2.
0x07 = LR3.
0x09 = LF2.
0x0A = LF1.
0x0C = OL1A.
0x0D = OL1C.
0x0E = OL2.
0x0F = OL3.</td></tr>
<tr><td rowspan="2">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Server</td><td colspan="2">Host</td></tr>
<tr><td>Nonvola-tile System Event Log</td><td>System Error Indicator</td><td>Event Log</td><td>E-Mail</td><td>Call-Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td></td><td></td><td>✔</td><td></td><td></td><td></td><td>✔</td></tr>
</table>

Event Code: 586	
Message:	`Invalid primitive sequence received for current link state.`
Severity:	Major.
Explanation:	The incident node has recognized either a Link-Reset (LR) or a Link-Reset_Response (LRR) Primitive Sequence while in the Wait-for-OLS state (see FC-PH clauses 16.5.4.3).
Action:	A Link-incident Record (LIR) is generated and sent to the host using the Link-Incident reporting procedure defined in the T11/99-017v0 document. If, after fault isolation is performed by the host, it is determined that the incident is because of a port failure, perform a data collection procedure for this switch using HAFM, Save the data file to the HAFM server Zip drive, and return the Zip disk to HP Services for analysis.

Event Data:	Byte **0** = Port number (00-8F). Bytes **4–7** = Elapsed millisecond tick count. Bytes **8–11** = Port state indicators: 0x00 = Active. 0x01 = OLIB. 0x05 = LR1. 0x06 = LR2. 0x07 = LR3. 0x09 = LF2. 0x0A = LF1. 0x0C = OL1A. 0x0D = OL1C. 0x0E = OL2. 0x0F = OL3.						
Distribution:	Switch		HAFM Server			Host	
	Nonvola-tile System Event Log	System Error Indicator	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
			✔				✔

SBAR Events (600 through 699)

In the Edge Switch 2/32, the SBAR is not a separate assembly, therefore not a FRU. It is an integral part of the switch's main circuit board. SBAR failure requires replacement of the entire switch.

Event Code: 602	
Message:	`SBAR module anomaly detected.`
Severity:	Informational.
Explanation:	Indicates that the control processor has detected a deviation in the normal operating mode or operating status of the indicated SBAR module.
Action:	No action required. There will be an additional event generated (604) if this event results in an SBAR logic failure.

<table>
<tr><td>Event Data:</td><td colspan="7">Byte 0 = Slot position.
Byte 1 = Anomaly reason code (See following chart).
Bytes 4–7 = Elapsed millisecond tick count.
Bytes 8–9 = High Availability error callout #1.
Bytes 10–11 = High Availability error callout #2.
Byte 12 = Detecting port.
Byte 13 = Connected port.
Byte 14 = Participating SBAR.
Bytes 16–17 =.High Availability error callout #3.
Bytes 18–19 =.High Availability error callout #4.</td></tr>
<tr><td rowspan="2">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Server</td><td colspan="2">Host</td></tr>
<tr><td>Nonvola-tile System Event Log</td><td>System Error Indicator</td><td>Event Log</td><td>E-Mail</td><td>Call-Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td></td><td>✔</td><td></td><td>✔</td><td></td><td></td><td></td><td></td></tr>
</table>

Event #602 Anomaly Reason Codes		
Reason Code	**Description**	**Additional Data**
0x00	Utility bus error to SBAR	HA Error Callouts (Words 2 and 4)
0x01	Utility bus error to Port Module	HA Error Callouts (Words 2 and 4)
0x02	Reserved	HA Error Callouts (Words 2 and 4)
0x03	SBAR module detected utility bus parity error	HA Error Callouts (Words 2 and 4)
0x04	Port module detected utility bus parity error	HA Error Callouts (Words 2 and 4)
0x05	SBAR module detected clock frequency error	HA Error Callouts (Words 2 and 4)
0x06	Port module detected clock frequency error	HA Error Callouts (Words 2 and 4)
0x07	SBAR module detected CTP interface signal error	HA Error Callouts (Words 2 and 4)

0x08	Port module detected CTP interface signal error	HA Error Callouts (Words 2 and 4)
0x09	SBAR Module detected external parity error	HA Error Callouts (Words 2 and 4)
0x0A	Port Module detected external parity error	HA Error Callouts (Words 2 and 4)
0x0B	SBAR Module detected lost of system clock	HA Error Callouts (Words 2 and 4)
0x0C	Port Module detected lost of system clock	HA Error Callouts (Words 2 and 4)
0x0D	SBAR detected invalid request from port	HA Error Callouts (Words 2 and 4)
0x0E	Internal SBAR time out	HA Error Callouts (Words 2 and 4)
0x0F	Internal SBAR parity error	HA Error Callouts (Words 2 and 4)
0x10	User port internal protocol error	HA Error Callouts (Words 2 and 4)
0x11	User port internal parity error	HA Error Callouts (Words 2 and 4)
0x12	User port internal buffer range error	HA Error Callouts (Words 2 and 4)
0x13	User port internal time out #1	HA Error Callouts (Words 2 and 4)
0x14	User port internal time out #2	HA Error Callouts (Words 2 and 4)
0x15	User port internal frame error—bad delimiter	HA Error Callouts (Words 2 and 4)
0x16	User port internal frame error—CRC	HA Error Callouts (Words 2 and 4)
0x17	User port internal frame error—invalid size	HA Error Callouts (Words 2 and 4)
0x18	User port internal frame error—long frame	HA Error Callouts (Words 2 and 4)
0x19	User port internal frame error—short frame	HA Error Callouts (Words 2 and 4)
0x1A	User port internal parity error	HA Error Callouts (Words 2 and 4)
0x1B	Buffer error	HA Error Callouts (Words 2 and 4)
0x1C	User port detected unexpected frame transmission	HA Error Callouts (Words 2 and 4)
0x1D	User port internal frame error—invalid trailer	HA Error Callouts (Words 2 and 4)

0x1E	User port detected frame internal integrity error	HA Error Callouts (Words 2 and 4)
0x1F	Internal connection time out	HA Error Callouts (Words 2 and 4)
0x20	User port detected elastic store error	HA Error Callouts (Words 2 and 4)
0x21	User port detected trailer parity error	HA Error Callouts (Words 2 and 4)
0x22	User port detected internal frame error—long frame	HA Error Callouts (Words 2 and 4)
0x23	Port detected SBAR response error	HA Error Callouts (Words 2 and 4)
0x24	User port detected clock error	HA Error Callouts (Words 2 and 4)
0x25	Port module internal address bus error	HA Error Callouts (Words 2 and 4)
0x26	User module internal data bus error	HA Error Callouts (Words 2 and 4)
0x27	User Port detected invalid address	HA Error Callouts (Words 2 and 4)
0x28	Embedded port detected frame integrity error	HA Error Callouts (Words 2 and 4)
0x29	Embedded port detected frame error—non-parity	HA Error Callouts (Words 2 and 4)
0x2A	Embedded port detected frame error—parity	HA Error Callouts (Words 2 and 4)
0x2B	Embedded port detected invalid SBAR response	HA Error Callouts (Words 2 and 4)
0x2C	Embedded port detected receive frame parity error	HA Error Callouts (Words 2 and 4)
0x2D	Embedded port detected connection time out	HA Error Callouts (Words 2 and 4)
0x2E	Embedded port detected receive fame overrun error	HA Error Callouts (Words 2 and 4)
0x2F	Embedded port detected frame transmit error	HA Error Callouts (Words 2 and 4)
0x30	Embedded port detected request time out	HA Error Callouts (Words 2 and 4)
0x31	Embedded port internal parity error	HA Error Callouts (Words 2 and 4)

0x32	Reserved (Engineering use only)	HA Error Callouts (Words 2 and 4)
0x33	Health Check—port failed busy bit clear	HA Error Callouts (Words 2 and 4)
0x34	Health Check—port detected bit synchronization error	HA Error Callouts (Words 2 and 4)
0x35	Diagnostic port test failure	HA Error Callouts (Words 2 and 4)
0x36	Embedded Port detected internal frame error—invalid trailer	HA Error Callouts (Words 2 and 4)
0x37	SBAR detected request out of range error	HA Error Callouts (Words 2 and 4)
0x38	User port internal time-out #3	HA Error Callouts (Words 2 and 4)
0x39	Embedded Port detected CRC Error	HA Error Callouts (Words 2 and 4)
0x3A	User port internal protocol error—Unsolicited response	HA Error Callouts (Words 2 and 4)
0x3B	User port detected frame error—Undeliverable frame	HA Error Callouts (Words 2 and 4)
0x3C	User port detected transmission rate discrepancy	HA Error Callouts (Words 2 and 4)
0x3D	User port detected transmission rate inconsistent mode	HA Error Callouts (Words 2 and 4)
0x3E	User port internal protocol error—Credit out of sync	HA Error Callouts (Words 2 and 4)
0x3F	Reserved	
0x40	SBAR detected request out of range error	HA Error Callouts (Words 2 and 4)
0x41	Reserved	
0x42	User egress port detected frame transmission error	HA Error Callouts (Words 2 and 4)
0x43	User ingress port detected internal time-out	HA Error Callouts (Words 2 and 4)
0x44	Reserved	HA Error Callouts (Words 2 and 4)
0x45	User egress port detected frame internal integrity error	HA Error Callouts (Words 2 and 4)

0x46	User egress port detected internal protocol error.	HA Error Callouts (Words 2 and 4)
0x47	User port detected internal frame length error	HA Error Callouts (Words 2 and 4)
0x48	User port detected internal buffer error	HA Error Callouts (Words 2 and 4)
0x49	User port detected internal queue protocol error.	HA Error Callouts (Words 2 and 4)
0x4A-0xFF		

<table>
<tr><th colspan="8">Event Code: 604</th></tr>
<tr><td>Message:</td><td colspan="7">SBAR module failure.</td></tr>
<tr><td>Severity:</td><td colspan="7">Major.</td></tr>
<tr><td>Explanation:</td><td colspan="7">A failure criteria associated with the serial crossbar hardware module has been met.</td></tr>
<tr><td>Action:</td><td colspan="7">Perform the data collection procedure for the switch using HAFM, save the data file to the HAFM server Zip drive, and return the Zip disk to HP Services for analysis.</td></tr>
<tr><td>Event Data:</td><td colspan="7">Byte 0 = Slot position.
Byte 1 = Reason code:
00 = Operator requested with debug command.
02 = Initialization failure.
03 = Hot plug/power up diagnostics failure acknowledgement.
04 = Communications with hardware is irregular or nonexistent.
05 = Read of module ID failed.
06 = High availability statistical error threshold reached.
07 = Communication with hardware is irregular or nonexistent.
Bytes 4–7 = Elapsed millisecond tick counter.
Bytes 8–11 = Reason code specific data.</td></tr>
<tr><td rowspan="2">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Server</td><td colspan="2">Host</td></tr>
<tr><td>Nonvolatile System Event Log</td><td>System Error Indicator</td><td>Event Log</td><td>E-Mail</td><td>Call-Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td></td><td>✔</td><td>✔</td><td>✔</td><td>✔</td><td>✔</td><td>✔</td><td></td></tr>
</table>

<table>
<tr><th colspan="8">Event Code: 605</th></tr>
<tr><td>Message:</td><td colspan="7">SBAR module revision not supported.</td></tr>
<tr><td>Severity:</td><td colspan="7">Minor.</td></tr>
<tr><td>Explanation:</td><td colspan="7">The specified SBAR module is not recognized by the existing firmware. The SBAR module will appear uninstalled to system software.</td></tr>
<tr><td>Action:</td><td colspan="7">Ensure that the switch model supports the operating firmware. If the firmware supports the model, perform the data collection procedure for the switch using HAFM. If the problem persists following a system power-on reset, replace the switch and return the switch and the Zip disk to HP Services for analysis and repair.</td></tr>
<tr><td>Event Data:</td><td colspan="7">Byte 0 = Slot position.
Bytes 4–7 = Elapsed millisecond tick counter.
Bytes 8–9: = Detected Module identifier.</td></tr>
<tr><td rowspan="2">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Server</td><td colspan="2">Host</td></tr>
<tr><td>Nonvolatile System Event Log</td><td>System Error Indicator</td><td>Event Log</td><td>E-Mail</td><td>Call-Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td></td><td>✔</td><td></td><td>✔</td><td></td><td></td><td></td><td></td></tr>
</table>

Thermal Events (800 through 899)

Event Code: 800							
Message:	`High-temperature warning (Port module thermal sensor).`						
Severity:	Major.						
Explanation:	The thermal sensor associated with the port module has detected that the "warm" temperature threshold level has been surpassed.						
Action:	Perform the data collection procedure for the switch using HAFM, Save the data file to the HAFM server Zip drive, and return the Zip disk to HP Services for analysis. Perform a system power-on reset. If the problem persists, replace the switch.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	Nonvolatile System Event Log	System Error Indicator	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 801	
Message:	`Critically hot temperature warning (Port module thermal sensor).`
Severity:	Major.
Explanation:	The thermal sensor associated with the port module has detected that the "hot" temperature threshold level has been surpassed.
Action:	Perform the data collection procedure for this switch using HAFM, Save the data file to the HAFM server Zip drive, and return the Zip disk to HP Services for analysis. Perform a system power-on reset. If the problem persists, replace the switch.
Event Data:	No supplementary data included with this event.

Distribution:	Switch		HAFM Server			Host	
	Nonvolatile System Event Log	System Error Indicator	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 802							
Message:	`Port module shutdown due to thermal violations.`						
Severity:	Major.						
Explanation:	The Port Module has been marked failed and power has been removed from the board due to excessive heat. This event follows an indication that the port module "hot" threshold level has been surpassed (event 801).						
Action:	Perform the data collection procedure for this switch using HAFM, Save the data file to the HAFM Zip drive, and return the Zip disk to HP Services for analysis. Perform a system power-on reset. If the problem persists, replace the switch.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	Nonvolatile System Event Log	System Error Indicator	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 810	
Message:	`High temperature warning (CTP card thermal sensor).`
Severity:	Major.
Explanation:	The thermal sensor associated with a CTP card indicates the warm temperature threshold was reached or exceeded.
Action:	Replace the failed switch. Perform the data collection procedure and return the Zip disk and faulty switch to HP support personnel.
Event Data:	No supplementary data included with this event.

Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error Indicator	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 805							
Message:	`High-temperature warning (SBAR module thermal sensor).`						
Severity:	Major.						
Explanation:	The thermal sensor associated with the SBAR module has detected that the "warm" temperature threshold level has been surpassed.						
Action:	Perform the data collection procedure for this switch using HAFM, Save the data file to the HAFM Zip drive, and return the Zip disk to HP Services for analysis. Perform a system power-on reset. If the problem persists, replace the switch.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	Nonvolatile System Event Log	System Error Indicator	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 807	
Message:	`SBAR module shutdown due to thermal violation.`
Severity:	Major.
Explanation:	The SBAR Module has been marked failed and power has been removed from the module due to excessive heat. This event follows an indication that the SBAR module "hot" threshold level has been surpassed (event 806).
Action:	Perform the data collection procedure for this switch using HAFM, Save the data file to the HAFM Zip drive, and return the Zip disk to HP Services for analysis. Perform a system power-on reset. If the problem persists, replace the switch.
Event Data:	No supplementary data included with this event.

Distribution:	Switch		HAFM Server			Host	
	Nonvolatile System Event Log	System Error Indicator	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 806							
Message:	`Critically hot temperature warning (SBAR module thermal sensor).`						
Severity:	Major.						
Explanation:	The thermal sensor associated with the SBAR module has detected that the "hot" temperature threshold level has been surpassed.						
Action:	Perform the data collection procedure for this switch using HAFM, Save the data file to the HAFM Zip drive, and return the Zip disk to HP Services for analysis. Perform a system power-on reset. If the problem persists, replace the switch.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	Nonvolatile System Event Log	System Error Indicator	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 811	
Message:	`Critically hot temperature warning (CTP card thermal sensor).`
Severity:	Major.
Explanation:	The thermal sensor associated with a CTP card indicates the hot temperature threshold was reached or exceeded.
Action:	Replace the failed switch. Perform the data collection procedure and return the Zip disk and faulty switch to HP support personnel.

Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 812							
Message:	`CTP card shutdown due to thermal violation.`						
Severity:	Major.						
Explanation:	A CTP failed and was powered off because of excessive heat. This event follows an indication that the hot temperature threshold was reached or exceeded (event code **811**).						
Action:	Replace the failed switch. Perform the data collection procedure and return the Zip disk and faulty switch to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Event Code: 850							
Message:	`System shutdown due to CTP card thermal violations.`						
Severity:	Severe.						
Explanation:	The switch powered off because of excessive thermal violations on the CTP card.						
Action:	Replace the failed switch. Perform the data collection procedure and return the Zip disk and faulty switch to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Server			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Glossary

This glossary defines terms used in this manual or related to this product and is not a comprehensive glossary of computer terms.

NUMERICS

8B/10B
A data encoding scheme developed by IBM, translating byte-wide data to an encoded 10-bit format.

10BaseT
An implementation of the Institute of Electrical and Electronics Engineers (IEEE) Ethernet standard on 24-gauge unshielded twisted-pair wiring, a baseband medium at 10 Mbps.

100BaseT
An implementation of the Institute of Electrical and Electronics Engineers (IEEE) Ethernet standard on 24-gauge unshielded twisted-pair wiring, a baseband medium at 100 Mbps.

A

AC
See alternating current.

access
The ability and means necessary to store data in, to retrieve data from, to transfer data into, to communicate with, or to make use of any resource of a storage device, a system, or area such as random access memory (RAM) or a register.

access control
A list of all devices that can access other devices across the network and the permissions associated with that access. *See also* persistent binding; zoning.

access time
The amount of time, including seek time, latency, and controller time, necessary for a storage device to retrieve information.

active configuration
In S/390 mode, the director or switch configuration that is determined by the status of the connectivity attributes.

active field-replaceable unit
Active FRU. A FRU that is currently operating as the active, and not the backup FRU. *See also* backup field-replaceable unit.

active FRU
See active field-replaceable unit.

active port address matrix
In S/390 mode, an active port address matrix is the port address matrix that is currently active or operational on an attached director or switch. *See also* connectivity capability.

active zone set
A single zone set that is active in a multiswitch fabric and is created when a specific zone set is enabled. This zone set is compiled by checking for undefined zones or aliases. *See also* zone; zone set.

address
(1) To refer to a device or an item of data by its address *(A, I)*. (2) The location in a computer where data is stored. (3) In data communication, the unique code assigned to each device or workstation connected to a network. (4) The identifier of a location, source, or destination *(D)*.

address name
Synonym for port name.

agent
Software that processes queries on behalf of an application and returns replies.

alarm
(1) A notification of an abnormal condition within a system that provides an indication of the location or nature of the abnormality to either a local or remote alarm indicator. (2) A simple network management protocol (SNMP) message notifying an operator of a network or device problem.

alert panel
This panel, located below the navigation control panel, displays an alert symbol that indicates the current state of the switch.

alias
A nickname representing a world-wide name.

allowed connection
In S/390 mode, in a director or switch, the attribute that when set, establishes dynamic connectivity capability. *Contrast with* blocked connection. *See* connectivity attribute. *See also* dynamic connectivity; unblocked connection.

allowed port connection
In S/390 mode, this attribute establishes dynamic connectivity capability.

alternating current
AC. Electric current that reverses direction at regular sinusoidal intervals *(D). Contrast with* direct current.

American National Standard Code for Information Interchange
ASCII. A standard character set consisting of 7-bit coded characters (8-bit including parity check) used for information exchange between systems and equipment *(D).*

American National Standards Institute
ANSI. A national organization consisting of producers, consumers, and general interest groups that establishes procedures by which accredited organizations create and maintain industry standards in the United States *(A).*

ANSI
See American National Standards Institute.

API
See application program interface.

application
(1) The use to which a data processing system is put, for example, a payroll application, an airline reservation application, or a network application. (2) A collection of software components used to perform specific types of work on a computer *(D).*

application client
The source object of the small computer system interface (SCSI) commands and destination for the command responses.

application program
(1) A program that is specific to the solution of an application problem. Synonymous with application software. (2) A program written for or by a user that applies to the user's work, such as a program that does inventory control or payroll. (3) A program used to connect and communicate with stations in a network, enabling users to perform application-oriented activities *(I).*

application program interface
API. A set of programming functions and routines that provides access between protocol layers, such as between an application and network services.

application-specific integrated circuit
ASIC. An asynchronous transfer mode (ATM) local area network/ wide area network (LAN/WAN) circuit using cell relay transport technology. ASICs are designed for a specific application or purpose, such as implementing the lower-layer Fibre Channel protocol (FC-0). They are particularly suited to sending video and audio information, as well as text. ASICs differ from general-purpose devices such as memory chips or microprocessors.

archive
(1) To copy files to a long-term storage medium for backup. (2) Removing data, usually old or inactive files, from a system and permanently storing the data on removable media to reclaim system hard disk space.

area
The second byte of the node port (N_Port) identifier.

ASCII
See American National Standard Code for Information Interchange.

ASIC
See application-specific integrated circuit.

attribute
In S/390 mode, the connection status of the address on a configuration matrix: allowed, blocked, or prohibited.

audit log
Log summarizing actions (audit trail) made by the user. There are two types of audit logs: the director or switch audit log, and the HAFM audit log.

(1) Director or switch audit log. Log displayed through the *Product Manager* application that provides a history of all configuration changes made to an individual director or switch from the respective *Product Manager* application, a simple network management protocol (SNMP) management workstation, a Fibre Connection (FICON) or open systems host, or the maintenance port. This information is useful for administrators and users. *Contrast with* HAFM audit log. *See also* Event Log; Hardware Log; Link Incident Log; Threshold Alert Log.

(2) *See* HAFM audit log.

availability
The accessibility of a computer system or network resource.

B

b
See bit.

B
See byte.

backbone
Cable on which two or more stations or networks may be attached, typically used to link computer networks at one site with those at another. Smaller branch networks are sometimes called ribs.

backplane
The backplane provides direct current (DC) power distribution and connections for all logic cards.

backup field-replaceable unit
Backup FRU. When an active FRU fails, an identical backup FRU takes over operation automatically (failover) to maintain director or switch and Fibre Channel link operation. *See also* active field-replaceable unit.

backup FRU
See backup field-replaceable unit.

bandwidth
(1) The amount of data that can be sent over a given circuit. (2) A measure of how fast a network can move information, usually measured in Hertz (Hz).

baud
The unit of signaling speed, expressed as the maximum number of times per second the signal can change the state of the transmission line or other medium. The units of baud are seconds to the negative 1 power. Note: With Fibre Channel scheme, a signal event represents a single transmission bit.

BB_Credit
See buffer-to-buffer credit.

beaconing
Use of light-emitting diodes (LEDs) on ports, port cards, field-replaceable units (FRUs), and switches to aid in the fault-isolation process. When enabled, active beaconing will cause LEDs to flash in order for the user to locate field-replaceable units (FRU's), switches, or directors in cabinets or computer rooms.

ber
See bit error rate.

bezel
A removable panel that covers empty drive bays and port cards.

bidirectional
In Fibre Channel protocol, the capability to simultaneously communicate at maximum speeds in both directions over a link.

bit
Abbreviated as b. (1) Binary digit, the smallest unit of data in computing, with a value of zero or one *(D)*. (2) A bit is the basic data unit of all digital computers. It is usually part of a data byte or data word; however, a single bit can be used to control or read logic ON/OFF functions. (3) A bit is a single digit in a binary number. Bits are the basic unit of information capacity on a computer storage device. Eight bits equals one byte.

bit density
Expressed as bits per inch (bpi), the number of bits that can be written on one inch of track on a disk surface.

bit error rate
Abbreviated as ber. Ratio of received bits that contain errors to total of all bits transmitted.

bits per inch
Abbreviated as bpi. Indicates the density of information on a hard drive.

blocked connection
In S/390 mode, in a director or switch, the attribute that, when set, removes the communication capability of a specific port. A blocked address is disabled so that no other address can be connected to it. A blocked attribute supersedes a dedicated or prohibited attribute on the same address. *Contrast with* allowed connection; unblocked connection. *See* connectivity attribute. *See also* dynamic connection; dynamic connectivity.

blocked port
In a director or switch, the attribute that when set, removes the communication capability of a specific port. A blocked port continuously transmits the offline sequence.

boot
(1) To start or restart a computer. (2) Loading the operating system.

bpi
See bits per inch.

B_Port
See bridge port.

bps
Bits per second.

Bps
Bytes per second.

bridge
(1) An attaching device that connects two local area network (LAN) segments to allow the transfer of information from one LAN segment to the other. A bridge can connect the LAN segments directly by network adapters and software in a single device, or can connect network adapters in two devices through software and use of a telecommunication link between the two adapters. (2) A functional unit that connects two LANs that use the same logical link control protocol, but may use different media access control protocols *(T)*. *Contrast with* router. (3) A device that connects and passes packets between two network segments that use the same communications protocol.

bridge port
B_Port. (1) In Fibre Channel protocol, a fabric inter-element port used to connect bridge devices with E_Ports on a switch. B_Ports provide a subset of E_Port functionality. (2) A term for a physical interface between the fabric (switch) and a bridge device. The interface is identical to an expansion port (E_Port), but it does not participate in full expansion port protocols. As such, it does not assign domain IDs or participate in routing protocol. *See also* expansion port; fabric port; generic port; node port; segmented expansion port.

British thermal unit
Btu. The quantity of heat required to raise the temperature of one pound of water by one degree Fahrenheit *(D)*.

broadband
Large bandwidth communications channel capable of multiple, parallel high-speed transmissions.

broadcast
In Fibre Channel protocol, to send a transmission to all node ports (N_Ports) on a fabric. *See also* broadcast frame.

broadcast frame
In Fibre Channel protocol, a frame whose destination address specifies all node ports (N_Ports) in the fabric. *See also* broadcast.

Btu
See British thermal unit.

buffer
Storage area for data in transit. Buffers compensate for differences in processing speeds between devices. *See* buffer-to-buffer credit.

buffer-to-buffer credit
BB_Credit. (1) The maximum number of receive buffers allocated to a transmitting node port (N_Port) or fabric port (F_Port). Credit represents the maximum number of outstanding frames that can be transmitted by that N_Port or F_Port without causing a buffer overrun condition at the receiver. (2) The maximum number of frames a port can transmit without receiving a receive ready signal from the receiving device. BB_Credit can be adjustable to provide different levels of compensation.

bypassed port
If a port is bypassed, all serial channel signals route past the port. A device attached to the port cannot communicate with other devices in the loop.

byte
Abbreviated as B. A byte generally equals eight bits, although a byte can equal from four to ten bits. A byte can also be called an octet *See also* octet.

C

call-home
Product feature which enables the HAFM server to automatically contact a support center and report system problems. The support center server accepts calls from the HAFM server, logs reported events, and can notify one or more support center representatives.

cascade
Linking two or more Fibre Channel switches to form a larger switch or fabric. The switched link through fiber cables attached between one or more expansion ports (E_Ports). *See also* expansion port.

CBY
Channel operations running in byte mode. This occurs when a channel is attached to a converter and specifies the I/O operation mode for the channel path under the I/O configuration program (IOCP) channel path identifier (CHPID) statement 'Type' parameter. *Contrast with* CVC.

cell
In S/390 mode, in a port address matrix, a cell is the intersection point between a horizontal port address and a vertical port address. A selected cell is indicated by the cell cursor.

chained
Two directors or switches that are physically attached.

channel
(1) A system element that controls one channel path, and whose mode of operation depends on the type of hardware attached. Each channel controls an I/O interface between the channel control element and the attached control units *(D)*. (2) Point-to-point link that transports data from one point to the other. (3) A connection or socket on the motherboard to controller card. A motherboard may have only one or two channels (primary and secondary). If a motherboard has only one channel, it may be necessary to add a controller card to create a secondary channel.

channel-attached
(1) Pertaining to direct attachment of devices by data I/O channels to a computer. (2) Pertaining to devices attached to a control unit by cables, not telecommunication lines *(D)*. *Synonymous with* local.

channel wrap test
A diagnostic procedure that checks S/390 host-to-director or host-to-switch connectivity by returning the output of the host as input. The test is host-initiated and transmits Fibre Channel frames to a director or switch port. A director or switch port enabled for channel wrapping echoes the frame back to the host.

Class 2 Fibre Channel service
Provides a connectionless (not dedicated) service with notification of delivery or nondelivery between two node ports (N_Ports).

Class 3 Fibre Channel service
Provides a connectionless (not dedicated) service without notification of delivery or nondelivery between two node ports (N_Ports). *Synonymous with* datagram.

Class F Fibre Channel service
Used by switches to communicate across interswitch links (ISLs) to configure, control, and coordinate a multiswitch fabric.

Class of Fibre Channel service
Defines the level of connection dedication, acknowledgment, and other characteristics of a connection.

command
(1) A character string from an external source to a system that represents a request for system action. (2) A request from a terminal to perform an operation or execute a program. (3) A value sent through an I/O interface from a channel to a control unit that specifies the operation to be performed *(D)*.

communications tray
The communications tray is a sliding tray located in the middle of the Fabricenter cabinet. The communications tray holds the laptop personal computer (PC), zip drive, and zip drive power supply.

community name (SNMP)
A name that represents an simple network management protocol (SNMP) community that the agent software recognizes as a valid source for SNMP requests. A product recognizes a management station as a valid recipient for trap information when the station's community names are configured.

community profile
Information that specifies which management objects are available to what management domain or simple network management protocol (SNMP) community name.

community (SNMP)
A relationship between an simple network management protocol (SNMP) agent and a set of SNMP managers that defines authentication, access control, and proxy characteristics.

component
(1) Hardware or software that is part of a functional unit. (2) A functional part of an operating system; for example, the scheduler or supervisor *(D)*.

concurrent firmware upgrade
Firmware is upgraded without disrupting switch operation.

concurrent maintenance
Ability to perform maintenance tasks, such as removal or replacement of field-replaceable units (FRUs), while a hardware product is operating.

configuration data
The collection of data that results from configuring product and system operating parameters. For example, configuring operating parameters, simple network management protocol (SNMP) agent, zoning configurations, and port configurations through the *Product Manager* application, results in a collection of configuration data. Configuration data includes: identification data, port configuration data, operating parameters, simple network management protocol (SNMP) configuration, and zoning configuration. A configuration backup file is required to restore configuration data if the control processor (CTP) card in a nonredundant Director 2/64 is removed and replaced.

connectionless
Nondedicated link. Typically used to describe a link between nodes which allows the switch to forward Class 2 or Class 3 frames as resources (ports) allow. Contrast this with the dedicated bandwidth that is required in a Class 1 Fibre Channel Service (FC-1) point-to-point link.

connectivity
The ability of devices to link together.

connectivity attribute
In S/390 mode, the characteristic that determines port address status for the director or switch. *See* allowed connection; blocked connection; connectivity capability; connectivity control; dynamic connection; dynamic connectivity; unblocked connection.

connectivity capability
(1) The capability that allows attachment of a device to a system without requiring physical reconfiguration of either the device or the interconnections. (2) The director or switch capability that allows logical manipulation of link connections to provide physical device attachment *(D)*. *See also* active port address matrix; connectivity attribute; connectivity control.

connectivity control
In S/390 mode, in a director or switch, the method used to change port address connectivity attributes and determine the communication capability of the link attached to the port *(D)*. *See also* active port address matrix; connectivity attribute; connectivity capability.

connector
Synonym for optical fiber connector.

console
See personal computer; server.

control processor card
CTP card. Circuit card that contains the director or switch microprocessor. The CTP card also initializes hardware components of the system after power-on. The card may contain an RJ-45 twisted pair connector. In the Edge Switch 2/16 and Edge Switch 2/32, the CTP card is the main circuit board of the switch and is not replaceable (not a FRU).

credit
See buffer-to-buffer credit.

CTP card
See control processor card.

customer support
Synonym for technical support.

CVC
Channel operations running in block mode. This occurs when a channel is attached to a converter. This specifies the I/O operation mode for the channel path under the I/O configuration program (IOCP) channel path identifier (CHPID) statement Type parameter. *Contrast with* CBY.

D

database
A collection of data with a given structure for accepting, storing, and providing on-demand data for multiple users. *(T)*

data directory
Critical information for all managed products (including directors and switches). Information stored here includes:

- All configuration data
- All log files
- Call-home settings
- Firmware library
- Zoning library

datagram
Synonym for Class 3 Fibre Channel service.

dB
See decibel.

dBm
Decibels referenced to one milliwatt. Zero dBm equals one milliwatt, with a logarithmic relationship as the value increases *(D)*.

DC
See direct current.

decibel
Abbreviated as dB. A standard unit used to express gain or loss of optical power, expressed as the ratio of input power to output power on a logarithmic basis *(D)*.

default
Pertaining to an attribute, value, or option that is assumed by a system when none is explicitly specified *(D, I)*.

default zone
A zone that contains all attached devices that are not members of a separate active zone.

destination
A point or location, such as a processor, director or switch, or server, to which data is transmitted *(D)*.

device
(1) Mechanical, electrical, or electronic hardware with a specific purpose *(D)*. *See also* managed product.

(2) *See* node.

diagnostics
(1) The process of investigating the cause or nature of a problem in a product or system. (2) Procedures or tests used by computer users and service personnel to diagnose hardware or software problems *(D)*.

dialog box
A pop-up window in the user interface with informational messages or fields to be modified or completed with desired options.

direct current
DC. Electric current that continuously flows in one direction *(D)*. *Contrast with* alternating current.

director
An intelligent, highly available, Fibre Channel switch providing any-to-any port connectivity between nodes (end devices) on a switched fabric. The director sends data transmissions (data frames) between nodes in accordance with the address information present in the frame headers of those transmissions.

diskette
A thin magnetic disk enclosed in a plastic jacket, which is removable from a computer and is used to store and transport data *(D)*.

diskette drive
The hardware mechanism by which a computer reads data from and writes data to removable diskettes *(D)*.

DNS name
Domain name system or domain name service. Host or node name for a device or managed product that is translated to an Internet protocol (IP) address through a domain name server.

domain
A Fibre Channel term describing the most significant byte in the node port (N_Port) identifier for the Fibre Channel device. It is not used in the Fibre Channel small computer system interface (FC-SCSI) hardware path ID. It is required to be the same for all SCSI targets logically connected to a Fibre Channel adapter.

domain ID
Domain identifier. A number that uniquely identifies a switch in a multiswitch fabric. A distinct domain ID is automatically allocated to each switch in the fabric by the principal switch. The preferred domain ID is the domain ID value that a switch requests from the principal switch. If the value has not been allocated to another switch in the fabric, it will be granted by the principal switch and will become the requesting switch's active domain ID. The active domain ID is the domain ID that has been assigned by the principal switch and that a switch is currently using.

domain name server
In TCP/IP, a server program that supplies name-to-address translation by mapping domain name to internet addresses. *(D)*

DRAM
See dynamic random access memory.

drop-down menu
A menu that displays when a heading in a navigation bar is clicked on with the mouse. The objects listed in the drop-down menus are organize by their headings in the navigation bar.

duplex
In data communication, pertaining to transmission in which data is sent and received at the same time *(D)*. *Contrast with* half duplex.

duplex connector
An optical fiber component that terminates jumper cable fibers in one housing and provides physical keying for attachment to a duplex receptacle *(D)*.

duplex receptacle
A fixed or stationary optical fiber component that provides a keyed attachment method for a duplex connector *(D)*.

dynamic connection
A connection between two ports, established or removed by the directors and that, when active, displays as one continuous link. *See* connectivity attribute. *See also* allowed connection; blocked connection; connectivity capability; dynamic connectivity; unblocked connection.

dynamic connectivity
The capability that allows connections to be established and removed at any time.

dynamic random access memory
DRAM. Random access memory that resides in a cell comprised of a capacitor and transistor. DRAM data deteriorates (that is, is dynamic) unless the capacitor is periodically recharged by the controlling microprocessor. DRAM is slow, but relatively inexpensive *(D)*. *Contrast with* static random access memory.

E

EAF
See enhanced availability feature.

EDI
See electronic data interchange.

E_D_TOV
See error-detect time-out value.

EE-PROM
See electronically erasable programmable read-only memory.

HAFM audit log
HAFM audit log. Log displayed though the *HAFM* application that provides a history of user actions performed at the HAFM server through the *HAFM* application. This information is useful for system administrators and users. *See also* audit log; HAFM Event Log; HAFM Product Status Log; HAFM Session Log.

HAFM Event Log
HAFM *Event Log*. Log displayed though the *HAFM* application that provides a record of events or error conditions recorded by the *HAFM Services* application. Entries reflect the status of the application and managed directors and switches. Information associated with a call-home failure is intended for use by maintenance personnel to fault isolate the problem (modem failure, no dial tone, etc.), while information provided in all other entries is generally intended for use by third-level support personnel to fault isolate more significant problems. *See also* HAFM audit log; HAFM Product Status Log; HAFM Session Log; Event Log.

***HAFM* application**
HP StorageWorks *High Availability Fabric Manager* (*HAFM*) application. (1) Software application that is the system management framework providing the user interface for managing Fibre Channel connectivity products. (2) The software application that implements the management user interface for all managed hardware products. The *HAFM* application can run both locally on the HAFM server and remotely on a user workstation.

HAFM Product Status Log
Log displayed though the *HAFM* application that records an entry when the status of a director or switch changes. The log reflects the previous status and current status of a managed product, and indicates the instance of a *Product Manager* application that should be opened to investigate a problem. The information is useful to maintenance personnel for fault isolation and repair verification. *See also* HAFM audit log; HAFM Event Log; HAFM Session Log.

HAFM server
HAFM server. A laptop shipped with the product for the purpose of running the *HAFM* application and *HAFM Services* applications.

HAFM Session Log
HAFM *Session Log*. Log displayed though the *HAFM* application that records a session (login and logout) history for the HAFM server, including the date and time, user name, and network address of each session. This information is useful for system administrators and users. *See also* HAFM audit log; HAFM Event Log; HAFM Product Status Log.

EIA
See Electronic Industries Association.

electromagnetic interference
EMI. Undesirable electromagnetic emissions generated by solar activity, lightning, and electronic devices. The emissions interfere with or degrade the performance of another electronic device *(D)*.

electronically erasable programmable read-only memory
A memory chip that can be loaded with data and later erased and loaded with update information.

electronic data interchange
EDI. The electronic transfer of preformatted business documents, such as purchase orders and bills of lading, between trading partners.

Electronic Industries Association
EIA. The governing body that publishes recommended standards for physical devices and associated interfaces. For example, RS-232 is the EIA standard that defines computer serial port connectivity *(D)*. *See also* Telecommunications Industry Association.

electronic mail
E-mail. Any communications service that permits the electronic transmission and storage of messages and attached or enclosed files.

electrostatic discharge
ESD. The undesirable discharge of static electricity that can damage or degrade electronic circuitry *(D)*.

e-mail
See electronic mail.

Embedded Web Server interface
The interface provides a graphical user interface (GUI) similar to the *Product Manager* application, and supports director or switch configuration, statistics monitoring, and basic operations. With director or switch firmware installed, administrators or operators with a browser-capable personal computer (PC) and an Internet connection can monitor and manage the director or switch through an Embedded Web Server interface.

Embedded Web Server interface timeout
If the Embedded Web Server interface is running but no user activity occurs, (such as viewing different pages, refreshing, or reconfiguring information), the application times out after 30 minutes. The user must log in again. A login dialog box displays if the user attempts to access any pages after the timeout has occurred.

Embedded Web Server interface window
The window for the Embedded Web Server interface. The window is divided into two separate panels: the navigation panel on the left, and the main panel on the right.

EMI
See electromagnetic interference.

enhanced availability feature
EAF. A backup field-replaceable unit (backup FRU) that is ordered and installed to provide redundancy and reduce disruption in case of failure.

enterprise
The entire storage system. The series of computers employed largely in high-volume and multi-user environments such as servers or networking applications; may include single-user workstations required in demanding design, engineering and audio/visual applications.

E_Port
See expansion port.

error-detect time-out value
E_D_TOV is the time the switch waits for an expected response before declaring an error condition.

error log
See Event Log.

error message
Indication that an error has been detected *(D)*.

ESD
See electrostatic discharge.

Ethernet
A widely implemented local area network (LAN) protocol that uses a bus or star topology and serves as the basis for the Institute of Electrical and Electronics Engineers (IEEE) 802.3 standard, which specifies the physical and software layers.

Ethernet hub
A device used to connect the HAFM server and the directors it manages.

event code
A three-digit number that specifies the exact event that occurred. This code provides information on system failures, such as hardware failures, failure locations, or general information on normal system events.

Event Log
Record of significant events that have occurred on the director or switch (director or switch Event Log) or through the *HAFM Services* application (HAFM Event Log). There are two *Event Logs*: director or switch *Event Log*, and *HAFM Event Log*.

(1) Director or switch *Event Log*. Log displayed through the *Product Manager* application that provides a history of events for an individual director or switch, such as system events, degraded operation, FRU failures, FRU removals and replacements, port problems, Fibre Channel link incidents, and HAFM server-to-product communication problems. All detected software and hardware failures are recorded in the *Event Log*. The information is useful to maintenance personnel for fault isolation and repair verification. *Contrast with* HAFM Event Log. *See also* audit log; Hardware Log; Link Incident Log; Threshold Alert Log.

(2) See HAFM Event Log.

exchange
A term that refers to one of the Fibre Channel protocol "building blocks," composed of one or more nonconcurrent sequences.

expansion port
E_Port. Physical interface on a Fibre Channel switch within a fabric, that attaches to an E_Port on another Fibre Channel switch through an interswitch link (ISL) to form a multiswitch fabric. *See also* bridge port; fabric port; generic port; node port; segmented expansion port.

F

fabric
Entity that interconnects node ports (N_Ports) and is capable of routing (switching) Fibre Channel frames, using the destination ID information in the Fibre Channel frame header accompanying the frames. A switch is the smallest entity that can function as a complete switched fabric topology.

fabric element
Any active director, switch, or node in a switched fabric.

fabric login
The process by which node ports (N_Ports) establish their operating parameters. During fabric login, the presence or absence of a fabric is determined, and paths to other N_Ports are mapped. Specific operating characteristics for each port, such as buffer-to-buffer credit (BB_Credit) and data frame size, are also established.

fabric login command
FLOGI. The command that establishes the initial operating parameters and topology for a fabric. The command is accepted by a fabric port (F_Port).

fabric mode
See interoperability mode.

fabric port
F_Port. Physical interface within the fabric that connects to a node port (N_Port) through a point-to-point full duplex connection. *See also* bridge port; expansion port; generic port; node port; segmented expansion port.

fabric services
The services that implement the various Fibre Channel protocol services that are described in the standards. These services include the fabric controller (login server), name server, and management server.

failover
Automatic and nondisruptive transition of functions from an active field-replaceable unit (FRU) that has failed to a backup FRU.

FC
See Fibre Channel.

FC-0
The Fibre Channel layer that describes the physical link between two ports, including the transmission media, transmitter and receiver circuitry, and interfaces *(D)*. This consists of a pair of either optical fiber or electrical cables (link media) along with transceiver circuitry which work together to convert a stream of bits at one end of the link to a stream of bits at the other end.

FC-1
Middle layer of the Fibre Channel physical and signaling interface (FC-PH) standard, defining the 8B/10B encoding/decoding and transmission protocol.

FC-2
The Fibre Channel layer that specifies the signaling protocol, rules, and mechanisms required to transfer data blocks. The FC-2 layer is very complex and provides different classes of service, packetization, sequencing, error detection, segmentation, and reassembly of transmitted data *(D)*.

FC-3
The Fibre Channel layer that provides a set of services common across multiple node ports (N_Ports) of a Fibre Channel node. The services are not commonly used and are essentially reserved for Fibre Channel architecture expansion *(D)*.

FC-4
The Fibre Channel layer that provides mapping of Fibre Channel capabilities to upper level protocols (ULP), including Internet protocol (IP) and small computer system interface (SCSI) *(D)*.

FCA
See Fibre Channel Association.

FC adapter
Fibre Channel adapter. *See* host bus adapter.

FCC
Federal Communications Commission.

FCC-IOC
See Fibre Channel I/O controller.

FCFE
See Fibre Channel fabric element.

FCFE-MIB
See Fibre Channel fabric element management information base.

FCIA
See Fibre Channel Industry Association.

FC IP
See Fibre Channel IP address.

FCMGMT
See Fibre Channel management framework integration.

FC-PH
See Fibre Channel physical and signaling interface.

feature key
A unique key to enable additional product features. This key is entered into the Configure Feature Key dialog box in the *Product Manager* application to activate optional hardware and software features. Upon purchasing a new feature, HP will provide the feature key to the customer.

fiber
The fiber-optic cable made from thin strands of glass through which data in the form of light pulses is transmitted. It is used for high-speed transmissions over medium (200 m) to long (10 km) distances.

fiber-optic cable
Synonym for optical cable.

fiber optics
The branch of optical technology concerned with the transmission of radiant power through fibers of transparent materials such as glass, fused silica, or plastic *(E)*. Telecommunication applications of fiber optics use optical fibers. A single fiber or a nonspatially aligned fiber bundle is used for each information channel. Such fibers are often called optical fibers to differentiate them from fibers that are used in noncommunication applications *(D)*.

fibre
A generic Fibre Channel term used to cover all transmission media types specified in the Fibre Channel Physical Layer (FC-PH) standard such as optical fiber, copper twisted pair, and copper coaxial cable.

Fibre Channel
FC. Integrated set of standards recognized by American National Standards Institute (ANSI) which defines specific protocols for flexible information transfer. Logically, a point-to-point serial data channel, structured for high performance.

Fibre Channel adapter
FC adapter. *See* host bus adapter.

Fibre Channel address
A 3-byte node port (N_Port) identifier which is unique within the address domain of a fabric. Each port may choose its own identifier, or the identifier may be assigned automatically during fabric login.

Fibre Channel Association
FCA. The FCA is a non-profit corporation consisting of over 150 members throughout the world. Its mission is to nurture and help develop the broadest market for Fibre Channel products through market development, education, standards monitoring, and fostering interoperability among members' products.

Fibre Channel fabric element
FCFE. Any device linked to a fabric.

Fibre Channel fabric element management information base
FCFE-MIB. A table of variables available to network management stations and resident on a switch or director. Through the simple network management protocol (SNMP) these pointers can be manipulates to monitor, control, and configure the switch or director.

Fibre Channel Industry Association
FCIA. A corporation consisting of over 100 computer industry-related companies. Its goal is to provide marketing support, exhibits, and tradeshows for its member companies. The FCIA complements activities of the various standards committees.

Fibre Channel I/O controller
FCC-IOC. In a director, the integrated controller on the control processor (CTP) card dedicated to the task of managing the embedded Fibre Channel port. In a director or switch, the FCC-IOC controls the embedded Fibre Channel port and configures the ports' application-specific integrated circuits (ASICs).

Fibre Channel IP address
FC IP. The default FC IP on a new switch is a temporary number divided by the switch's world-wide name (WWN). The system administrator needs to enter a valid IP address.

Fibre Channel management framework integration
FCMGMT. A standard defined by the Fibre Alliance to provide easy management for Fibre Channel-based devices such as switches, hubs, and host-bus adapters.

Fibre Channel physical and signaling interface
FC-PH. The American National Standards Institute (ANSI) document that specifies the FC-0 (physical signaling), FC-1 (data encoding), and FC-2 (frame construct) layers of the Fibre Channel protocol *(D)*.

Fibre Channel standard
American National Standards Institute (ANSI) standard that provides a common, efficient data transport system that supports multiple protocols. The architecture integrates both channel and network technologies, and provides active, intelligent interconnection among devices. All data transmission is isolated from the control protocol, allowing use of point-to-point, arbitrated loop, or switched fabric topologies to meet the needs of an application.

Fibre Connection
FICON. An IBM set of products and services introduced in 1999 that is based on the Fibre Channel Standard. FICON technology uses fiber-optic cables as the data transmission medium, and significantly improves I/O performance (including one Gbps bi-directional data transfer). FICON is designed to coexist with ESCON™ channels, and FICON-to-ESCON control unit connections are supported.

FICON
See Fibre Connection.

FICON Management server
An optional feature that can be enabled on the director or switch or switch through the *Product Manager* application. When enabled, host control and management of the director or switch or switch is provided through an S/390 Parallel Enterprise or 2/Series server attached to a director or switch or switch port.

field-replaceable unit
FRU. Assembly removed and replaced in its entirety when any one of its components fails *(D)*. *See* active field-replaceable unit.

file server
A computer that stores data centrally for network users and manages access to that data.

file transfer protocol
FTP. A transmission control protocol/Internet protocol (TCP/IP) —based client/server protocol used to transfer files to and from a remote host. Does not perform any conversion or translation.

firewall
A networking device that blocks unauthorized access to all or parts of a network.

firewall zoning
Hardware enforced access between F_Ports enforced at the source port. The hardware verifies the destination port against the zone defined for the source port.

firmware
Embedded program code that resides and runs on, for example, directors, switches, and hubs.

FLASH memory
Reusable nonvolatile memory that is organized as segments for writing, and as bytes or words for reading. FLASH memory is faster than read-only memory, but slower than random access memory *(D)*.

FLOGI
See fabric login command.

F_Port
See fabric port.

frame
A variable-length packet of data that is transmitted in frame relay technology.

FRU
See field-replaceable unit.

FTP
See file transfer protocol.

full-duplex
The capability to transmit in two directions simultaneously.

G

gateway address
(1) In transmission control protocol/Internet protocol (TCP/IP), a device that connects two systems that use the same or different protocols. (2) In TCP/IP, the address of a router to which a device sends frames destined for addresses not on the same physical network (for example, not on the same Ethernet) as the sender. The hexadecimal format for the gateway address is XXX.XXX.XXX.XXX.

Gb
See gigabit.

GB
See gigabyte.

Gbps
Acronym for gigabits per second.

generic port
G_Port. Physical interface on a director or switch that can function either as a fabric port (F_Port) or an expansion port (E_Port), depending on the port type to which it connects. *See also* bridge port; expansion port; fabric port; node port; segmented expansion port.

GHz
See gigahertz.

gigabit
Gb. A unit of measure for data storage, equal to approximately 134,217,728 bytes. Approximately one eighth of a gigabyte.

gigabyte
GB. A unit of measure for data storage, equal to 1,073,741,824 bytes. Generally approximated as one billion bytes *(D)*.

gigahertz
GHz. One billion cycles per second (Hertz) *(D)*.

G_Port
See generic port.

graphical user interface
GUI. A visually oriented interface where the user interacts with representations of real-world objects displayed on the computer screen. Interactions with such objects produce actions that are intuitive to the user *(D)*.

ground
That portion of a conducting circuit connected to the earth *(D)*.

GSM card
A generic port (G_Port) module card containing shortwave laser ports for multimode fiber-optic cables.

GUI
See graphical user interface.

H

half duplex
The capacity to transmit in two directions, but not simultaneously.

hardware
Physical equipment (director, switch, or personal computer) as opposed to computer programs or software.

Hardware Log
Director or switch *Hardware Log*. Log displayed through the *Product Manager* application that provides a history of FRU removals and replacements (insertions) for an individual director or switch. The information is useful to maintenance personnel for fault isolation and repair verification. *See also* audit log; Event Log; Link Incident Log; Threshold Alert Log.

HBA
See host bus adapter.

Hertz
Hz. A unit of frequency equal to one cycle per second.

heterogeneous fabric
A fabric containing open-fabric-compliant products from various vendors. *Contrast with* homogeneous fabric.

hexadecimal
A numbering system with base of sixteen; valid numbers use the digits 0 through 9 and characters A through F, where A represents 10 and F represents 15 *(D)*.

high availability
A performance feature characterized by hardware component redundancy and concurrent maintenance. High-availability systems maximize system uptime while providing superior reliability, availability, and serviceability.

homogeneous fabric
A fabric consisting of only one vendor's products. *Contrast with* heterogeneous fabric.

hop
(1) Data transfer from one node to another node. (2) Describes the number of switches that handle a data frame from its origination point through it's destination point.

hop count
The number of hops a unit of information traverses in a fabric.

host bus adapter
HBA. Logic card that provides a link between the server and storage subsystem, and that integrates the operating systems and I/O protocols to ensure interoperability.

host processor
(1) A processor that controls all or part of a user application network *(T)*. (2) In a network, the processing unit in which resides the access method for the network *(D)*.

hot pluggable
See concurrent maintenance.

hot spare
See field-replaceable unit.

hot swap
See concurrent maintenance.

hot-swapping
See concurrent maintenance.

HTTP
See hypertext transport protocol.

hub
(1) In Fibre Channel protocol, a device that connects nodes into a logical loop by using a physical star topology. (2) In Ethernet, a device used to connect the HAFM server and the directors it manages.

hyperlink
A predefined link for jumping from one location to another, within the same computer or network site or even to a location at a completely different physical location. Commonly used on the world wide web for navigation, reference, and depth where published text will not suffice.

hypertext transport protocol
HTTP. A simple protocol that allows world wide web pages to be transferred quickly between web browsers and servers.

Hz
See Hertz.

I

ID
See identifier.

identifier
ID. (1) One or more characters used to identify or name a data element and possibly to indicate certain properties of that data element *(D, T)*. (2) A sequence of bits or characters that identifies a program, device, or system to another program, device, or system. *See also* port name.

IEEE
See Institute of Electrical and Electronics Engineers.

IML
See initial machine load.

inband management
Management of the director or switch through Fibre Channel. An interface connection to a port card. *Contrast with* out-of-band management.

initial machine load
IML. Hardware reset for all installed control processor (CTP) cards on the director or switch. This reset does not affect other hardware. It is initiated by pushing the IML button on a director's or switch's operating panel.

initial program load
IPL. The process of initializing the device and causing the operating system to start. An IPL may be initiated through a menu option or a hardware button.

initial program load configuration
IPL configuration. In S/390 mode, information stored in a director or switch's nonvolatile memory that contains default configurations. The director or switch loads the file for operation when powered on.

Institute of Electrical and Electronics Engineers
IEEE. An organization of engineers and technical professionals that promotes the development and application of electronic technology and allied sciences.

integrated product
Hardware product that is mounted in the Fabricenter cabinet. For example, any director or switch shipped with in the Fabricenter cabinet is an integrated product.

interface
(1) A shared boundary between two functional units, defined by functional, signal, or other characteristics. The concept includes the specification of the connection of two devices having different functions *(T)*. (2) Hardware, software, or both, that link systems, programs, or devices *(D)*.

Internet protocol
IP. Network layer for the transmission control protocol/Internet protocol (TCP/IP) protocol used on Ethernet networks. IP provides packet routing, fragmentation, and reassembly through the data link layer *(D)*.

Internet protocol address
IP address. Unique string of numbers (in the format xxx.xxx.xxx.xxx) that identifies a device on a network.

interoperability
Ability to communicate, execute programs, or transfer data between various functional units over a network.

interoperability mode
Interop mode. An operating mode set through management software that allows products to operate in homogeneous or heterogeneous fabrics.

interop mode
See interoperability mode.

interrupt
A signal sent by a subsystem to the central processing unit (CPU) that signifies a process has either completed or could not be completed.

interswitch link
ISL. Physical expansion port (E_Port) connection between two directors in a fabric.

interswitch link hop
ISL hop. *See* hop.

IOPS
Input/output operations per second.

IP
See Internet protocol.

IP address
See Internet protocol address.

IPL
See initial program load.

IPL configuration
See initial program load configuration.

ISL
See interswitch link.

ISL hop
Interswitch link hop. *See* hop.

isolated E_Port
Isolated expansion port. *See* segmented expansion port.

isolated expansion port
Isolated E_Port. *See* segmented expansion port.

ITE
Information technology equipment.

J

Java
An object-oriented programming language derived from C++ that produces code that is platform independent. Developed by Sun Microsystems designed for distribution and distributable applications development. Java applications require a program called the Java Virtual Machine (JVM) to execute. JVMs have been developed for many of the mainstream platforms and operating systems.

jumper cable
Optical cable that provides physical attachment between two devices or between a device and a distribution panel. *Contrast with* trunk cable. *See also* optical cable.

K

Kb
See kilobit.

KB
See kilobyte.

kilobit
Kb. A unit of measure for data storage, equaling 1,024 bits, or two to the tenth power. Kilobits are generally approximated as being one thousand bits.

kilobyte
KB. A unit of measure for data storage, equaling 1,024 bytes, or two to the tenth power. Kilobytes are generally approximated as being one thousand bytes.

L

laser
Laser is an acronym for light amplification by stimulated emission of radiation. A device that produces a very powerful narrow beam of coherent light of a single wavelength by simulating the emissions of photons from atoms, molecules, or ions.

latency
Amount of time elapsed between receipt of a data transmission at a switch's incoming fabric port (F_Port) from the originating node port (N_Port) to retransmission of that data at the switch's outgoing F_Port to the destination N_Port. The amount of time it takes for data transmission to pass through a switching device.

LCD
Liquid crystal display.

LED
See light-emitting diode.

light-emitting diode
LED. A semiconductor chip that emits visible or infrared light when electricity passes through it. LEDs are used on switch or director field-replaceable units (FRUs) and the front bezel to provide visual indications of hardware status or malfunctions.

LIN
See link incident.

link
Physical connection between two devices on a switched fabric. A link consists of two conductors, one used for sending and the other for receiving, thereby providing a duplex communication path.

link incident
LIN. Interruption to link due to loss of light or other causes. *See also* link incident alerts.

link incident alerts
A user notification, such as a graphic symbol in the *Product Manager* application **Hardware View** that indicates that a link incident has occurred. *See also* link incident.

Link Incident Log
Director or switch Link Incident Log. Log displayed through the *Product Manager* application that provides a history of Fibre Channel link incidents (with associated port numbers) for an individual director or switch. The information is useful to maintenance personnel for isolating port problems (particularly expansion port (E_Port) segmentation problems) and repair verification. *See also* audit log; Event Log; Hardware Log; Threshold Alert Log.

LMA
See loader/monitor area.

load balancing
Ability to evenly distribute traffic over multiple interswitch links within a fabric. Load balancing on HP directors and switches takes place automatically.

loader/monitor area
LMA. Code that resides in the loader/monitor area of the control processor (CTP) card. Among other functions, LMA code provides I/O functions available through the maintenance port, operator panel, server interface, terminal window command functions, power up diagnostics, field-replaceable unit (FRU) power-on hours update, and data read/write control, and LMA code/licensed internal code (LIC) download functions *(D)*.

local
Synonym for channel-attached.

logical partition
LPAR. A processor hardware subset defined to support the operation of a system control program, and can be used without affecting any of the applications in another partition *(D)*.

logical port address
In a director or switch, the address used to specify port connectivity parameters and to assign link addresses for the attached channels and control units.

logical switch number
LSN. A two-digit number used by the I/O configuration program (IOCP) to identify a director or switch *(D)*.

logical unit number
LUN. In Fibre Channel addressing, a logical unit number is a number assigned to a storage device which, in combination with the storage device's node port's world-wide name, represents a unique identifier for a logical device on a storage area network. Peripherals use LUNs to represent addresses. A small computer system interface (SCSI) device's address can have up to eight LUNs.

login server
Entity within the Fibre Channel fabric that receives and responds to login requests.

longwave
Lasers or light-emitting diodes (LEDs) that emit light with wavelengths around 1300 nm. When using single mode (9 nm) fiber, longwave lasers can be used to achieve lengths greater than 2 Km.

loopback plug
In a fiber optic environment, a type of duplex connector used to wrap the optical output signal of a device directly to the optical input. *Contrast with* protective plug. *Synonymous with* wrap plug.

loopback test
Test that checks attachment or control unit circuitry, without checking the mechanism itself, by returning the output of the mechanism as input.

LPAR
See logical partition.

LSN
See logical switch number.

LUN
See logical unit number.

M

MAC address
See media access control address.

main panel
(1) The rightmost frame of the windows in *HAFM* applications. (2) The rightmost frame of the Embedded Web Server interface window. *See also* navigation panel.

maintenance analysis procedure
MAP. A written or online set of procedures that guide maintenance personnel through step-by-step instructions for hardware fault isolation, repair, and verification *(D)*.

maintenance port
Connector on the director or switch where a PC running an American National Standard Code for Information Interchange (ASCII) terminal emulator can be attached or dial-up connection made for specialized maintenance support.

managed product
Hardware product that can be managed with the *HAFM* application. HP directors and switches are managed products. *See also* device.

management information base
MIB. Related set of software objects (variables) containing information about a managed device and accessed via simple network management protocol (SNMP) from a network management station.

management session
A session that exists when a user logs on to the *HAFM* application. HAFM can support multiple concurrent management sessions. The user must specify the network address of the *HAFM* application's server at logon time.

MAP
See maintenance analysis procedure.

matrix
See active port address matrix.

Mb
Megabit.

MB
See megabyte.

Mbps
Megabits per second.

MBps
Megabytes per second.

media access control address
MAC address. Hardware address of a node (device) connected to a network.

megabyte
MB. A unit of measure for data storage, equal to 1,048,576 bytes. Generally approximated as one million bytes.

memory
A device or storage system capable of storing and retrieving data.

menu
A list of items displayed on a monitor from which a user can make a selection.

menu bar
The menu bar is located across the top of a monitor window. Pull-down menus are displayed by clicking the menu bar option with the mouse, or by pressing **Alt** with the underlined letter of the name for the menu bar option *(D)*.

MIB
See management information base.

mirroring
The writing of data to pairs of drives in an array, creating two exact copies of the drive contents. This procedure provides a backup of data in case of a failure.

modem
Modem is an abbreviation for modulator/demodulator. A communication device that converts digital computer data to signals and signals to computer data. These signals can be received or transmitted by the modem via a phone line or other method of telecommunication.

ms
Millisecond.

multimedia
A simultaneous presentation of data in more than one form, such as by means of both visual and audio.

multimode optical fiber
A graded-index or step-index optical fiber that allows more than one mode (light path) to propagate. *Contrast with* singlemode optical fiber.

multiplexer
A device that allows two or more signals to be transmitted simultaneously on a single channel.

multiswitch fabric
Fibre Channel fabric created by linking more than one director or fabric switching device within a fabric.

N

name server
(1) In TCP/IP, *see* domain name server. (2) In Fibre Channel protocol, a server that allows node ports (N_Ports) to register information about themselves. This information allows N_Ports to discover and learn about each other by sending queries to the name server.

name server zoning
Node port (N_Port) access management that allows N_Ports to communicate if and only if they belong to a common name server zone.

NAS
See network-attached storage.

navigation panel
The left side of the Embedded Web Server interface window. Click words in this panel to display menu options. *See also* main panel.

network
An arrangement of hardware, software, nodes, and connecting branches that comprises a data communication system. The International Organization for Standardization (ISO) seven-layer specification partitions a computer network into independent modules from the lowest (physical) layer to the highest (application) layer *(D)*.

network address
Name or address that identifies a device on a transmission control protocol/Internet protocol (TCP/IP) network. The network address can be either an IP address in dotted-decimal notation (composed of four three-digit octets in the format xxx.xxx.xxx.xxx) or a domain name (as administered on a customer network).

network-attached storage
NAS. Storage connected directly to the network, through a processor and its own operating system. Lacks the processor power to run centralized, shared applications.

network interface card
NIC. An expansion board inserted into a computer so the computer can be connected to a network. Most NICs are designed for specific types of networks, protocols, and medias, although some can serve multiple networks.

network management
The broad subject of managing computer networks. There exists a wide variety of software and hardware products that help network system administrators manage a network. Network management covers a wide area, including security, performance, and reliability.

never principal
The setting that prevents the product from becoming the principal switch for a fabric.

NIC
See network interface card.

nickname
Alternate name assigned to a world-wide name for a node, director or switch in the fabric.

node
In Fibre Channel protocol, an end device (server or storage device) that is or can be connected to a switched fabric. *See also* device.

node port
N_Port. Physical interface within an end device that can connect to an fabric port (F_Port) on a switched fabric or directly to another N_Port (in point-to-point communications). *See also* bridge port; expansion port; fabric port; generic port; segmented expansion port.

node port identifier
N_Port ID. In Fibre Channel protocol, a unique address identifier by which an N_Port is uniquely known. It consists of a domain (most significant byte), an area, and a port, each 1 byte long. The N_Port ID is used in the source identifier (S_ID) and destination identifier (D_ID) fields of a Fibre Channel frame.

nondisruptive maintenance
See concurrent maintenance.

nonvolatile random access memory
NV-RAM. RAM that retains its content when the device power is turned off.

N_Port
See node port.

N_Port ID
See node port identifier.

NV-RAM
See nonvolatile random access memory.

O

octet
An 8-bit quantity, often called a byte or word. An octet can equal a byte as long as the byte equals eight bits. *See also* byte.

OEM
See original equipment manufacturer.

offline
Referring to data stored on a medium, such as tape or even paper, that is not available immediately to the user.

offline diagnostics
Diagnostics that only operate in stand alone mode. User operations cannot take place with offline diagnostics running.

offline sequence
OLS. (1) Sequence sent by the transmitting port to indicate that it is attempting to initialize a link and has detected a problem in doing so. (2) Sequence sent by the transmitting port to indicate that it is offline.

offline state
When the switch or director is in the offline state, all the installed ports are offline. The ports transmit an offline sequence (OLS) and they cannot accept a login got connection from an attached device. *Contrast with* online state.

ohm
A unit of electrical resistance equal to that of a conductor in which a current of one ampere is produced by a potential of one volt across the conductor terminals *(D)*.

OLS
See offline sequence.

online
Referring to data stored on the system so it is available immediately to the user.

online diagnostics
Diagnostics that can be run by the customer engineer while the operational software is running. These diagnostics do not impact user operations.

online state
When the switch or director is in the online state, all of the unblocked ports are allowed to log in to the fabric and begin communicating. Devices can connect to the switch or director if the port is not blocked and can communicate with another attached device if both devices are in the same zone, or if the default zone is enabled. *Contrast with* offline state.

Open Systems Architecture
OSI. A model that represents a network as a hierarchical structure of functional layers. Each layer provides a set of functions that can be accessed and used by the layer above. Layers are independent, in that implementation of a layer can be changed without affecting other layers *(D)*.

open systems management server
OSMS. An optional feature that can be enabled on the director or switch through the *Product Manager* application. When enabled, host control and management of the director or switch are provided through an Open System Interconnection (OSI) device attached to a director or switch port.

open systems mode
The mode that is used for HP or open fabrics. See also operating mode; S/390 mode.

operating mode
In directors or switches, in managed products, a selection between s/390 and open systems mode. *See also* open systems mode; S/390 mode.

operating system
OS. Software that controls execution of applications and provides services such as resource allocation, scheduling, I/O control, and data management. Most operating systems are predominantly software, but partial hardware implementations are possible *(D, T)*.

Operating System/390
OS/390™. An integrated, open-enterprise server operating system developed by IBM that incorporates a leading-edge and open communications server, distributed data and file services, parallel Sysplex™ support, object-oriented programming, distributed computing environment, and open application interfaces *(D)*.

optical cable
Single fiber, multiple fibers, or a fiber bundle in a structure built to meet optical, mechanical, and environmental specifications *(D, E)*. *See also* jumper cable; trunk cable. *Synonymous with* fiber-optic cable.

optical drive backup
A data backup system that uses rewriteable optical cartridges (ROCs) as the storage medium.

optical fiber connector
Synonymous with connector.

ordered set
In Fibre Channel protocol, four 10-bit characters (a combination of data and special characters) providing low-level link functions, such as frame demarcation and signaling between two ends of a link. It provides for initialization of the link after power-on and for some basic recovery functions.

original equipment manufacturer
OEM. A company that has a special relationship with computer producers. OEMs buy components and customize them for a particular application. They sell the customized computer under their own name. OEMs may not actually be the original manufacturers. They are usually the customizers and marketers.

OS
See operating system.

OS/390™
See Operating System/390.

OSI
See Open Systems Architecture.

OSMS
See open systems management server.

out-of-band management
Transmission of management information, using frequencies or channels other than those routinely used for information transfer.

P

packet
In Fibre Channel protocol, Logical unit of information (usually in the form of a data frame) transmitted on a network. It contains a header (with all relevant addressing and timing information), the actual data, and a trailer (which contains the error checking function, usually in the form of a cyclic redundancy check), and frequently user data.

panel
A logical component of the interface window. Typically, a heading and/or frame marks the panel as an individual entity of the window. Size and shape of the panel and its data depend upon the purpose of the panel and may or may not be modified.

PC
See personal computer.

persistent binding
A form of server-level access control that uses configuration information to bind a server to a specific Fibre Channel storage volume (or logical device), using a unit number. *See also* access control.

personal computer
PC. A portable computer that consists of a system unit, display, keyboard, mouse, one or more diskette drives, and internal fixed-disk storage *(D)*.

point-to-point
A Fibre Channel protocol topology that provides a single, direct connection between two communication ports. The director or switch supports only point-to-point topology.

port
Receptacle on a device to which a cable leading to another device can be attached. Ports provide Fibre Channel connections *(D)*.

port address name
A user-defined symbolic name of 24 characters or less that identifies a particular port address.

port authorization
Feature of the password definition function that allows an administrator to extend operator-level passwords to specific port addresses for each director or switch definition managed by a personal computer (PC). Port authorization affects only operator-level actions for active and saved matrices *(D)*.

port name
Name that the user assigns to a particular port through the *Product Manager* application. *See also* identifier. *Synonymous with* address name.

POST
See power-on self-test.

power-on self-test
POST. Series of diagnostic tests that are run automatically by a device when the power is turned on

preferred domain ID
Configured value that a switch will request from the Principal Switch. If the preferred value is already in use, the Principal Switch will assign a different value.

preventive service planning bucket
PSP bucket. Collected problems after early ship of an IBM product.

principal switch
In a multiswitch fabric, the switch that allocates domain IDs to itself and to all other switches in the fabric. There is always one principal switch in a fabric. If a switch is not connected to any other switches, it acts as its own principal switch.

printed wiring assembly
PWA. A thin board on which integrated circuits and other electronic components are placed and connected to each other via thin copper traces.

private device
A loop device that cannot transmit a fabric login command (FLOGI) command to a switch or director, nor communicate with fabric-attached devices. *Contrast with* .public device.

processor complex
A system configuration that consists of all the machines required for operation, for example, a processor unit, a processor controller, a system display, a service support display, and a power and coolant distribution unit.

Product Manager application
Application that implements the management user interface for a director or switch. There are two *Product Manager* applications: director or switch Product Manager, and HAFM Product Manager. (1) In the *HAFM Services* application, the software component that provides a graphical user interface for managing and monitoring HAFM products. When a product instance is opened from the *HAFM* application **Product View** or Fabric Manager **Topology View**, the corresponding HAFM *Product Manager* application is invoked.

product name
User-configurable identifier assigned to a managed product. Typically, this name is stored on the product itself. A director or switch product name can also be accessed by a simple network management protocol (SNMP) manager as the system name.

Product View
The top-level display in the HAFM software user interface that displays icons of managed products.

prohibited port connection
In a director or switch, in S/390 operating mode, an attribute that removes dynamic connectivity capability.

proprietary
Privately owned and controlled. In the computer industry, proprietary is the opposite of open. A proprietary design or technique is one that is owned by a company. It also implies that the company has not divulged specifications that would allow other companies to duplicate the product. Increasingly, proprietary architectures are seen as a disadvantage. Consumers prefer open and standardized architectures, which allow them to mix and match products from different manufacturers.

protective plug
In a fiber-optic environment, a type of duplex connector (or cover) that provides physical protection *(D)*. *Contrast with* loopback plug.

protocol
(1) Set of semantic and syntactic rules that determines the behavior of functional units in achieving communication. (2) In systems network architecture, the meanings of and sequencing rules for requests and responses for managing the network, transferring data, and synchronizing network component states. (3) A specification for the format and relative timing of data exchanged between communicating devices *(D, I)*.

.public device
A loop device that can transmit a fabric login command (FLOGI) to a switch, receive acknowledgement from the switch's login server, register with the switch's name server, and communicate with fabric-attached devices. Public devices communicate with fabric-attached devices through the switch's bridge port (B_Port) connection to a director or switch. *Contrast with* private device.

pull-down menu
See drop-down menu.

PWA
See printed wiring assembly.

R

radio frequency interference
RFI. Electromagnetic radiation which is emitted by electrical circuits carrying rapidly changing signals, as a by-product of the normal operation, and which causes unwanted signals (interference or noise) to be induced in other circuits.

RAM
See random access memory.

random access memory
RAM. A group of computer memory locations that is numerically identified to allow high-speed access by the controlling microprocessor. A memory location is randomly accessed by referring to its numerical identifier *(D)*. *Contrast with* read-only memory. *See* also dynamic random access memory; nonvolatile random access memory; static random access memory.

R_A_TOV
See resource allocation time-out value.

read-only memory
ROM. An information storage chip with permanent memory. Stored information cannot be changed or deleted except under special circumstances *(D)*. *Contrast with* random access memory.

redundancy
Performance characteristic of a system or product whose integral components are backed up by identical components to which operations will automatically failover in the event of a component failure. Redundancy is a vital characteristic of virtually all high-availability (24 hours/7 days per week) computer systems and networks.

remote notification
A process by which a system is able to inform remote users and workstations of certain classes of events that occur on the system. E-mail notification and the configuration of simple network management protocol (SNMP) trap recipients are two examples of remote notification programs that can be implemented on director-class switches.

remote user workstation
Workstation, such as a personal computer (PC), using *HAFM* application and *Product Manager* application software that can access the HAFM server over a local area network (LAN) connection.

repeater
A device that generates and often amplifies signals to extend transmission distance.

rerouting delay
An option that ensures that frames are delivered in order through the fabric to their destination.

resource allocation time-out value
R_A_TOV is a value used to time-out operations that depend on the maximum possible time that a frame could be delayed in a fabric and still be delivered.

RFI
See radio frequency interference.

ROM
See read-only memory. *Contrast with* random access memory.

router
An attaching device that connects two local area network (LAN) segments, which use similar or different architectures, at the reference model network layer *(D)*. *Contrast with* bridge.

RS-232
The Electronic Industry Association (EIA)-recommended specification for asynchronous serial interfaces between computers and communications equipment. It specifies both the number of pins and type of connection, but does not specify the electrical signals *(D)*.

S

S/390 mode
The mode that is most useful when attaching to IBM S/390 Enterprise servers. *See also* open systems mode; operating mode.

SA/MVS™
See System Automation for Operating System/390.

SAN
See storage area network; system area network.

SA OS/390™
See System Automation for Operating System/390.

scalable
Refers to how well a system can adapt to increased demands. For example, a scalable network system could start with just a few nodes but easily expands to thousands of nodes. Scalability is important because it allows the user to invest in a system with confidence that a business will not outgrow it. Refers to anything whose size can be changed.

SCSI
See small computer system interface.

segment
A fabric segments when one or more switches cannot join the fabric because of various reasons. The switch or switches remain as separate fabrics.

segmented E_Port
See segmented expansion port.

segmented expansion port
Segmented E_Port. E_Port that has ceased to function as an E_Port within a multiswitch fabric due to an incompatibility between the fabrics that it joins. *See also* bridge port; fabric port; generic port; node port.

serial port
A full-duplex channel that sends and receives data at the same time. It consists of three wires: two that move data one bit at a time in opposite directions, and a third wire that is a common signal ground wire.

server
A computer that provides shared resources, such as files and printers, to the network. Used primarily to store data, providing access to shared resources. Usually contains a network operating system.

SFP transceivers
See small form factor pluggable transceivers.

shortwave
Lasers or light-emitting diodes (LEDs) that emit light with wavelengths around 780 nm or 850 nm. When using multimode fiber (50 nm) shortwave lasers can be used with Fibre Channel links less than 500 m. To achieve longer lengths, single-mode fiber is required. The preferred fiber core size is 50 micron as this fiber has large bandwidth so that the distance is limited by the fiber attenuation. A 62.5 micron core size is also supported for compatibility with existing FDDI installations. Fiber of this type has smaller bandwidth and, in this case, the distance is limited by the fiber bandwidth.

simple mail transfer protocol
SMTP. A transmission control protocol/Internet protocol (TCP/IP) protocol that allows the user to create, send, and receive text messages. SMTP protocols specify how messages are passed across a link from one system to another. They do not specify how the mail application accepts, presents, or stores the mail.

simple network management protocol
SNMP. A transmission control protocol/Internet protocol (TCP/IP)-derived protocol governing network management and monitoring of network devices.

simple network management protocol community
SNMP community. Also known as SNMP community string. SNMP community is a cluster of managed products (in SNMP terminology, hosts) to which the server or managed product running the SNMP agent belongs.

simple network management protocol community name
SNMP community name. The name assigned to a given SNMP community. Queries from an SNMP management station to a device running an SNMP agent will only elicit a response if those queries are addressed with the correct SNMP community name.

simple network management protocol management station
SNMP management station. An SNMP workstation personal computer (PC) used to oversee the SNMP network.

simple network management protocol version 1
SNMP v1. The original standard for SNMP is now referred to as SNMP v1. The Edge Switch 2/16 and the Edge Switch 2/32 use SNMP v1.

simple network management protocol version 2
SNMP v2. The second version of the SNMP standard. This version expands the functionality of SNMP and broadens its ability to include OSI-based, as well as TCP/IP-based, networks as specified in RFC 1441 through 1452.

singlemode optical fiber
An optical fiber that allows one wavelength-dependent mode (light path) to propagate. *Contrast with* multimode optical fiber.

small computer system interface
SCSI. An interface standard that enables computers to communicate with peripherals connected to them. Commonly used in enterprise computing and in Apple Macintosh systems. Usually pronounced as "scuzzy." The equivalent interface in most personal computers is enhanced integrated drive electronics (EIDE).

A narrow SCSI adapter supports up to eight devices, including itself. SCSI address 7 has the highest priority followed by 6, 5, 4, 3, 2, 1, 0, with 0 being the lowest priority.

small form factor pluggable transceivers
SFP transceivers. Laser-based optical transceivers for a wide range of networking applications requiring high data rates. The transceivers, which are designed for increased densities, performance, and reduced power, are well-suited for Fibre Channel applications.

SMTP
See simple mail transfer protocol.

SNMP
See simple network management protocol.

SNMP community
See simple network management protocol community.

SNMP community name
See simple network management protocol community name.

SNMP management station
See simple network management protocol management station.

SNMP v1
See simple network management protocol version 1.

SNMP v2
See simple network management protocol version 2.

SRAM
See static random access memory.

SSP
See system services processor.

state
The state of the switch or director. Possible values include online, offline, testing, and faulty. See offline state; online state.

static random access memory
SRAM. SRAM is microprocessor-cache random access memory. It is built internal to the microprocessor or on external chips. SRAM is fast, but relatively expensive *(D)*. *Contrast with* dynamic random access memory.

storage area network
SAN. A high-performance data communications environment that interconnects computing and storage resources so that the resources can be effectively shared and consolidated.

stored addresses
In S/390 mode, a method for configuring addresses.

subnet
A portion of a network that shares a common address component. On transmission control protocol/Internet protocol (TCP/IP) networks, subnets are defined as all devices whose IP addresses have the same prefix. Dividing a network into subnets is useful for both security and performance reasons. IP networks are divided using a subnet mask.

subnet mask
A mask used by a computer to determine whether another computer with which it needs to communicate is located on a local or remote network. The network mask depends upon the class of networks to which the computer is connecting. The mask indicates which digits to look at in a longer network address and allows the router to avoid handling the entire address. Subnet masking allows routers to move the packets more quickly. Typically, a subnet may represent all the machines at one geographic location, in one building, or on the same local area network.

switch
A device that connects, filters and forwards packets between local area network (LAN) segments or storage area network (SAN) nodes or devices.

switchover
Changing a backup field-replaceable unit (FRU) to the active state, and the active FRU to the backup state.

switch priority
Value configured into each switch in a fabric that determines its relative likelihood of becoming the fabric's principal switch. Lower values indicate higher likelihood of becoming the principal switch. A value of 1 indicates the highest priority; 225 is the lowest priority. A value of 225 indicates that the switch is not capable of acting as the principal switch. The value 0 is illegal.

System Automation for Operating System/390
SA OS/390™. IBM licensed software that provides System/390 Parallel Sysplex™ management, automation capabilities, and integrated systems and network management. SA OS/390 manages host, remote processor, and I/O operations. SA OS/390 integrates the functions of Automated Operations Control for Multiple Virtual Storage (MVS™), ESCON™ Manager, and Target System Control Facility *(D)*.

system name
See product name.

system services processor
SSP. In a director or switch, the central controlling processor. Controls the RS-232 maintenance port and the Ethernet port of a Fibre Channel director or switch.

T

TB
See terabyte.

TCP
See transmission control protocol.

TCP/IP
See transmission control protocol/Internet protocol.

technical support
Single point of contact for a customer when assistance is needed in managing or troubleshooting a product. Technical support provides assistance twenty-four hours a day, seven days a week, including holidays. The technical support number is **(800) 652 6672**. *Synonymous with* customer support.

Telecommunications Industry Association
TIA. A member organization of the Electronic Industries Association (EIA), TIA is the trade group representing the communications and information technology industries. *See also* Electronic Industries Association.

telnet
The Internet standard protocol for remote terminal connection over a network connection.

terabyte
TB. One thousand (1,000) gigabytes; one terabyte of text on paper would consume 42,500 trees. At 12 characters per inch, 1 TB of data in a straight line would encircle the earth 56 times and stretch some 1.4 million miles equalling nearly three round trips from the earth to the moon.

Threshold Alert Log
Director or switch *Threshold Alert Log*. Log displayed through the *Product Manager* application that provides details of threshold alert notifications for an individual director or switch. The log displays the date and time an alert occurred, and displays details about the alert as configured for the product. The information is useful to maintenance personnel for fault isolation and repair verification. *See also* audit log; Event Log; Hardware Log; Link Incident Log.

TIA
See Telecommunications Industry Association.

topology
Logical and/or physical arrangement of stations on a network.

transceiver modules
Transceiver modules come in longwave, extra longwave, or shortwave laser versions, providing a single fiber connection.

transfer rate
The speed with which data can be transmitted from one device to another. Data rates are often measures in megabits (Mbps) or megabytes (MBps) per second, or gigabits (Gbps) or gigabytes per second (GBps).

transmission control protocol
TCP. The transport layer for the transmission control protocol/Internet protocol (TCP/IP) protocol widely used on Ethernet networks and any network that conforms to U.S. Department of Defense standards for network protocol. TCP provides reliable communication and control through full-duplex connections *(D)*.

transmission control protocol/Internet protocol
TCP/IP. A layered set of protocols (network and transport) that allows sharing of applications among devices on a high-speed local area network (LAN) communication environment *(D)*. *See also* transmission control protocol; Internet protocol.

trap
Unsolicited notification of an event originating from a simple network management protocol (SNMP) managed device and directed to an SNMP network management station.

trap host
Simple network management protocol (SNMP) management workstation that is configured to receive traps.

trap recipient
In simple network management protocol (SNMP), a network management station that receives messages through SNMP for specific events that occur on the arbitrated loop device.

trunk cable
Cable consisting of multiple fiber pairs that do not directly attach to an active device. This cable usually exists between distribution panels and can be located within, or external to, a building *(D)*. *Contrast with* jumper cable. *See also* optical cable.

U

UDP
See user datagram protocol.

UL
See Underwriters Laboratories.

ULP
See upper level protocol.

unblocked connection
In a director or switch, the absence of the blocked attribute for a specific port. *Contrast with* blocked connection. *See* connectivity attribute. *See also* allowed connection; dynamic connection; dynamic connectivity.

unblocked port
Devices communicating with an unblocked port can login to the director or switch and communicate with devices attached to any other unblocked port (assuming that this is supported by the current zoning configuration).

Underwriters Laboratories
UL. A laboratory organization accredited by the Occupational Safety and Health Administration and authorized to certify products for use in the home and workplace *(D)*.

unicast
Communication between a single sender and a single receiver over a network.

uninterruptable power supply
UPS. A buffer between public utility power or another power source, and a system that requires precise, uninterrupted power *(D)*.

UNIX
A popular multi-user, multitasking operating system originally designed to be a small, flexible system used exclusively by programmers. UNIX was one of the first operating systems to be written in a high-level programming language, namely C. This meant that it could be installed on virtually any computer for which a C compiler existed. Due to its portability, flexibility, and power, UNIX has become the leading operating system for workstations. Historically, it has been less popular in the personal computer market, but the emergence of a new version called Linux is revitalizing UNIX across all platforms.

upper level protocol
ULP. Protocols that map to and run on top of the Fibre Channel FC-4 layer. ULPs include Internet protocol (IP) and small computer system interface (SCSI).

UPS
See uninterruptable power supply.

user datagram protocol
UDP. A connectionless protocol that runs on top of Internet protocol (IP) networks. User datagram protocol/Internet protocol (UDP/IP) offers very few error recovery services, instead providing a direct way to send and receive datagrams over an IP network. UDP/IP is primarily used for broadcasting messages over an entire network. *Contrast with* transmission control protocol/Internet protocol.

V

VAC
See volts alternating current.

VDC
See volts direct current.

virtual machine
VM®. (1) A virtual data processing system that displays to be at the exclusive disposal of a single user, but whose functions are accomplished by sharing the resources of a real data processing system. (2) A functional simulation of a computer system and its associated devices, multiples of which can be controlled concurrently by one operating system *(D, T)*.

virtual storage
VS. (1) Storage space that may be regarded as addressable main storage by the user of a computer system in which virtual addresses are mapped to real addresses. The size of virtual storage is limited by the addressing scheme of the computer system and by the amount of auxiliary storage available, not by the number of main storage locations. (2) Addressable space that is apparent to the user as processor storage space, from which the instructions and the data are mapped to the processor storage locations *(A, D, I)*.

volt
A measure of the difference in electrical potential between two points in a conductor, equal to one ohm resistance carrying a constant current of one ampere, with a power dissipation of one watt *(D)*. *See* volts alternating current; volts direct current.

volts alternating current
VAC. A term for classifying the system in which volts exist. VAC means that the volts exist in a circuit where the electricity can travel in either direction. *Contrast with* volts direct current. *See* volt.

volts direct current
VDC. A term for classifying the system in which volts exist. VDC means that the electricity has a specific path it must follow. *Contrast with* volts alternating current. *See* volt.

W

warning message
A message that indicates a possible error has been detected. *See also* error message.

watt
A unit of power in the International System equal to one joule (Newton-meter) per second *(D)*.

window
The main window for the *HAFM* application or *Product Manager* applications. Each application has a unique window that is divided into separate panels for the title, navigation control, alerts, and the main or **Product View**. The user performs all management and monitoring functions for these Fibre Channel products through the application window.

workstation
A terminal or microcomputer usually connected to a network or mainframe at which a user can perform applications.

world-wide names
WWN. Eight-byte string that uniquely identifies a Fibre Channel entity (that is, a port, a node, a switch, a fabric), even on global networks.

wrap plug
Synonym for loopback plug.

wrap test
A test that checks attachment or control unit circuitry, without checking the mechanism itself, by returning the output of the mechanism as input. A wrap test can transmit a specific character pattern through a system and compare the pattern received with the pattern transmitted *(D)*.

write authorization
Permission for an simple network management protocol (SNMP) management station with the proper community name to modify writable management information base (MIB) variables.

WWN
See world-wide names.

Z

zip drive
A high capacity floppy disk and disk drive developed by the Iomega Corporation. Zip disks are slightly larger than conventional floppy disks. The storage capacity for zip disks is between 100 and 250 MB of data. The zip drive and disk is used for backing up the HAFM server, and is located on the communications tray behind the HAFM server.

zone
Set of devices that can access one another. All connected devices may be configured into one or more zones. Devices in the same zone can see each other. Those devices that occupy different zones cannot. *See also* active zone set; zone set; zoning.

zone member
Specification of a device to be included in a zone. A zone member can be identified by the port number of the director or switch to which it is attached or by its port world-wide name (WWN). In multiswitch fabrics, identification of end-devices or nodes by WWN is preferable.

zone set
A collection of zones that may be activated as a unit. *See also* active zone set; zone.

zoning
Grouping of several devices by function or by location. All devices connected to a connectivity product, such as the director or switch, may be configured into one or more zones. *See also* access control; zone.

Index

10/100 Mbps LAN connectors 1–12

A

additional port function 2–67
alert symbols
    HAFM 1–23
    Product Manager 1–27
alerts
    introduction 1–5
audit logs 3–6

B

bandwidth of ports 1–1
beaconing
    introduction 1–6
blocking a port 3–39

C

call home feature
    introduction 1–6
call-home notification
    reporting 1–43
CD-ROM
    drive 1–12
channel wrap test, procedure 3–29
circle, green
    meaning of 1–35
clock speed 1–12
configuration data
    backing up 3–49
    managing 3–48
    resetting 3–51
    restoring 3–50
connectors and indicators 1–19
CTP cards
    event codes tables B–20

D

data collection 1–6
diagnostic software
    introduction 1–6
diagnostics
    HAFM 1–21
    port 3–19
    Product Manager 1–24
    software 1–21
dialog boxes
    port properties 1–29
    switch properties 1–28
diamond, red
    meaning of 1–35
director
    firmware
        version 1–13
disk drive 1–12
domain ID 1–8
    zone member 3–18

E

E_Port segmentation 1–8
Edge Switch 2/32
    operating status 1–35
electrostatic discharge (ESD)
    repair procedures, caution 3–2
email messages
    introduction 1–6
e-mail notification
    reporting 1–43

Embedded Web Server 1–12
diagnostics 1–41
ESD
repair procedures, caution 3–2
Ethernet
hub 1–12
LAN, connector 1–20
ethernet LAN connectors 1–12
event codes
CTP card events B–20
description B–1
fan module events B–17
power supply events B–14
system events B–2
thermal events B–60
event log 3–6
external loopback tests 3–28

F

fabric logs 3–5
fabric manager
messages A–1
fabric tree 1–37
Fabrics Tab
zone sets view 3–17
fabrics view
topology tab, illustration 1–37
view area 1–37
zone sets tab, illustration 1–38
fan module events, event codes tables B–17
fans 1–18
illustrations 5–2
LEDs 1–20
part numbers 5–2
removal 4–6
replacement 4–7
fiber-optic
cleaning kit 1–45
components, cleaning 3–33
protective plug 1–44
wrap plug 1–44
Fibre Connection management server, see FMS
Fibre Connection, see FICON
FICON
product management 1–4
field replaceable units
See FRUs
firmware
adding a version 3–41
deleting a version 3–45
determining version 3–41
downloading 3–46
managing versions 3–40
modifying description 3–44
FMS
product management 1–4
FRU list view 1–31
displayed 1–31
FRUs 1–17
fans 1–18, 5–2
front-accessible 5–1
illustrations 5–1
part numbers 5–1
power supplies 1–19, 5–2
rear-accessible 5–2
RRPs 4–1
SFP transceivers 1–18, 5–1
status LEDs 1–20

G

gateway address
default 2–1, 3–2

H

HAFM
alert symbols 1–23
audit log 3–3
diagnostic features 1–21
event log 3–3
HAFM application
introduction 1–3
messages A–1
HAFM server
description 1–11
remote workstation 1–3

specifications 1–12
HAFM services
description 1–38
event table 1–39
status line 1–40
hard drive 1–12
hardware log 3–7
Hardware View 1–24, 3–20
hardware view 1–28
displayed 1–28
status conditions 1–28
status symbol function 1–28
using 1–28

I

illustrated parts breakdown 5–1
IML button 1–19
IML procedure 3–35
inactive port 2–67
inband management access methods 1–4
Intel Pentium processor 1–12
internal loopback tests 3–26
IP address
default 2–1, 3–2
IPL procedure 3–35

L

LAN
connector 1–20
LEDs
fan 1–20
FRU status 1–20
port 3–19
port SFPs 1–20
power supply 1–20
PWR LED 1–20
link incident log 3–9, 3–10
local area network
See LAN
logs
audit 3–6
event 3–6
fabric 3–5
HAFM audit 3–3
HAFM Event 3–3
hardware 3–7
introduction 1–5
link incident 3–9, 3–10
product status 3–5
session 3–4
using information 3–2
loopback tests
port, external 3–28
port, internal 3–26

M

maintenance
approach 1–13
event codes B–1
maintenance analysis procedures
See MAPs
maintenance port 1–6, 1–21
management
HAFM application 1–3
out-of-band 1–3
SNMP agent 1–3
switch 1–3
web server 1–3
MAP 0000-Start Map 2–7
MAP 0100-Power Distribution Analysis 2–26
MAP 0200-POST, Reset, or IPL Failure Analysis 2–32
MAP 0300-Console Application Problem Determination 2–33
MAP 0400-Loss of Console Communication 2–39
MAP 0500-Fan and CTP Card Failure Analysis 2–58
MAP 0600-Port Failure and Link Incident Analysis 2–63
MAP 0700-Fabric, ISL, and Segmented Port Problem Determination 2–79
MAP 0800-Console PC Problem Determination 2–90
MAPs 2–1

collecting data 3–32
event codes B–1
MAP 0000-Start Map 2–7
MAP 0100-Power Distribution Analysis 2–26
MAP 0200-POST, Reset or IPL Failure Analysis 2–32
MAP 0300-Console Application Problem Determination 2–33
MAP 0400-Loss of Console Communication 2–39
MAP 0500-Fan and CTP Card Failure Analysis 2–58
MAP 0600-Port Failure and Link Incident Analysis 2–63
MAP 0700-Fabric, ISL, and Segmented Port Problem Determination 2–79
MAP 0800-Console PC Problem Determination 2–90
quick start 2–1
memory
HAFM server 1–12
RAM 1–12
menu bar, description 1–24
menus
menu bar 1–24
node list view 1–32
performance view 1–34
port 1–29
port list view 1–30
switch 1–28
messages
fabric manager A–1
HAFM application A–1
Product Manager A–19
modem (external) 1–12
modem cable 1–44
multiswitch fabric 1–8
domain ID 1–8
E_Port segmentation 1–8
port segmentation 1–8
zoning 1–8

N

Node List View 3–16
node list view 1–32
node list view menu 1–32
nodes, types, list of 3–17
notebook PC 1–11
null modem cable 1–44

O

offline, setting switch 3–37
online, setting switch 3–37
open-system management server, see OSMS
operating status for the Edge Switch 2/32 1–35
OSMS
product management 1–4
out-of-band management
description 1–3

P

part numbers 5–1
parts 5–1
password
default 2–1, 3–2
PCMCIA slots 1–12
Pentium processor 1–12
Performance View 3–17
performance view menu 1–34
performance view option 1–33
personal computer, HAFM server 1–11
port
blocking 3–39
diagnostics 3–19
LEDs 3–19
loopback tests, external 3–28
loopback tests, internal 3–26
segmentation 1–8
swapping 3–30
unblocking 3–40
port bandwidth 1–1
Port List View 3–12
port list view
displayed 1–30

port list view menu 1–30
port menu 1–29
port properties dialog box 1–29
ports
displaying statistics 1–34
WWN, node list view 2–73
ports list view 1–30
power off procedure 3–35
power supplies 1–19
illustrations 5–2
LEDs 1–20
part numbers 5–2
removal 4–4
replacement 4–5
power supply events, event codes tables B–14
preventive maintenance, cleaning fiber-optic components 3–33
product management
FICON 1–4
FMS 1–4
inband access 1–4
OSMS 1–4
Product Manager
alert symbols 1–27
diagnostic features 1–24
Hardware View 1–24, 3–20
messages A–19
Node List View 3–16
Performance View 3–17, 3–23
Port List View 3–12
using views 3–12
product manager 1–28
FRU list view 1–31
menu bar 1–24
node list view 1–32
node list view menu 1–32
performance view 1–33
performance view menu 1–34
port list view 1–30
port menu 1–29
status bar 1–34
switch view 1–28
view panel 1–28
product status log 3–5
protective plug, fiber-optic 1–44

Q

quick start, MAPs 2–1

R

RAM 1–12
remote workstation
configurations 1–14
minimum specifications 1–16
repair, event codes B–1
RRPs 4–1
fans 4–6
power supplies 4–4
SFP transceivers 4–2

S

S/390 mode
channel wrap tests 3–19
procedure 3–29
enabling or disabling port channel wrapping 3–14
port channel wrapping, enabling and disabling 3–25
swapping Fibre Channel port address 3–25
swapping port addresses 3–14
swapping ports 3–30
safety
ESD
repair procedures 3–2
serviceability features 1–5
session log 3–4
SFP transceivers 1–18
illustrations 5–1
LEDs 1–20
longwave 1–18
part numbers 5–1
protective plug 1–44
removal 4–2
replacement 4–3
shortwave 1–18

wrap plug 1–44
simple network management protocol
See SNMP
SNMP
introduction 1–3, 1–7
trap message support 1–42
software
diagnostic features 1–21
installing 3–51
upgrading 3–51
specifications, remote workstations 1–16
specifications, switch 1–9
square, gray, meaning of 1–35
statistics on ports 1–34
status bar 1–34, 1–35
status bar symbols 1–35
status table 1–26
subnet mask
default 2–1, 3–2
swapping ports 3–30
switch
audit logs 3–6
connectors and indicators 1–19
description 1–2
error-detection, reporting, and serviceability features 1–5
event codes B–1
event log 3–6
fabric logs 3–5
fans 1–18
FRUs 1–17
FRUs, front accessible 5–1
FRUs, rear accessible 5–2
hardware log 3–7
illustrated parts breakdown 5–1
IML procedure 3–35
IPL procedure 3–35
LEDs 1–20
link incident log 3–9, 3–10
maintenance port 1–21
management 1–3
MAPs 2–1
multiswitch fabric 1–8
power off procedure 3–35
power supplies 1–19
setting offline 3–37
setting online 3–37
SFP transceivers 1–18
specifications 1–9
status table 1–26
tools supplied 1–44
zoning feature 1–7
switch menu 1–28
switch properties dialog box 1–28
symbols, status bar, table of 1–35
system events
event codes tables B–2

T

thermal events, event codes tables B–60
tools and test equipment 1–43
tools, supplied by service personnel 1–45
tools, supplied with switch 1–44
topology tab 1–37
illustration 1–37
transmission distance 1–1
triangle, yellow
meaning of 1–35

U

unblocking a port 3–40

V

versions
director firmware 1–13
Intel processor 1–12
Windows 2000 1–12
view area 1–37
view panel 1–28
views
Hardware 1–24, 3–20
Node List 3–16
Performance 3–17, 3–23
Port List 3–12
Zone sets 3–17

W

web server
introduction 1–3
Web Server, Embedded 1–12
Windows 2000 1–12
wrap plug, fiber-optic 1–44
WWN
node list view 2–73
WWN, zone member 3–18

Z

Zip drive 1–12
zone set
description of 1–7
zone set tab 1–38
zone sets tab, illustration 1–38
Zone sets View 3–17
zoning 1–7